دراسات

د. ماجد محمد الحنيطي

تكنولوجيا الصراعات الدولية المعاصرة



طُبع بدعم من وزارة الثقافة
2020


الآن ناشرون وموزعون



تكنولوجيا الصراعات الدولية المعاصرة

تكنولوجيا الصراعات الدولية المعاصرة

د. ماجد محمد الحنيطي

الطبعة الأولى 2021.



الآن ناشرون وموزعون

المدير العام: د. باسم الزعبي

الأردن، عمّان، شارع الملكة رانيا، عمارة المفلح التجاري (87)، ط1. هاتف: 797162720، 65620722(962+)

alaan. publish@gmail.com

alaanpublishers.com

المراجعة اللغوية: د. نزار فلوّح

التنسيق الفني: م. سجود العناسوة

تصميم الغلاف: بسام حمدان



الآراء الواردة في الكتاب لا تعبّر بالضرورة عن رأي الجهة الداعمة

ISBN: 978-9923-13-324-8

المملكة الأردنية الهاشمية

رقم الإيداع لدى دائرة المكتبة الوطنية

(2020/12/5288)

327.16

الحنيطي، ماجد

تكنولوجيا الصراعات الدولية المعاصرة/ ماجد محمد الحنيطي. عمان: الآن ناشرون وموزعون، 2020

() ص

ر.إ.: 2020/7/2631

الواصفات: / الصراعات الدولية// النزاعات المسلحة// التكنولوجيا الحديثة

يتحمل المؤلف كامل المسؤولية القانونية عن محتوى مصنفه ولا يعبر هذا المصنف عن رأي دائرة المكتبة الوطنية أو أي جهة حكومية أخرى.

د. ماجد محمد الحنيطي

تكنولوجيا الصراعات الدولية المعاصرة

دراسة



فهرس المحتويات

الفصل الأول

مفاهيم ونظريات متعلقة بتكنولوجيا الصراعات الدولية

الفصل الثاني

الثورة في تقنيات الحرب وتطبيقاتها في الصراعات الدولية

الفصل الثالث

حرب الفضاء الإلكتروني

الفصل الرابع

الحرب النفسية الإلكترونية

الفصل الخامس

أثر حرب الفضاء الإلكتروني على طبيعة العلاقات الدولية

إلى من أنار طريقي وصبر معي أكثر مما صبرت . . **والدي**

إلى التي باركت طريقي بصلاتها ودعواتها . . **والدتي**

تقديم

د. وليد عبد الهادي العويمر*

عندما تسلمت الدراسة التي أنجزها الدكتور ماجد الحنيطي والموسومة «تكنولوجيا الصراعات الدولية المعاصرة: الثورة في الشؤون العسكرية وحرب الفضاء الإلكتروني»، لفت انتباهي عنوان الدراسة الذي يختلف تمامًا عن العناوين التقليدية التي تتحدث بشكل مفصل عن الحرب الإلكترونية أو الصراعات الدولية المعاصرة كلًا على حدة.

ومكمن هذا الاختلاف هو محاولة الكاتب بيان العلاقة الارتباطية القوية بين التطورات التكنولوجية الحديثة من جهة، وتصاعد الصراعات الدولية في العصر الحديث وتنوّعها وتعدّدها من جهة أخرى، وهذا الترابط حاول الكاتب من خلاله أن يبين أنّ التطورات التقنية والتكنولوجية لها جوانب سلبية كثيرة، مثلما لها جوانب إيجابية عديدة أيضًا.

وقد ظهر تمكُّن الباحث من خلال إلمامه بالجانب النظري والبحث والتقصي في أحدث الكتب والدراسات التي تناولت التقنيات التكنولوجية الحديثة، والجانب العملي من خلال اطّلاعه على أبرز

* أستاذ العلوم السياسية، جامعة مؤتة، الأردن.

وأهم الأزمات والصراعات الإقليمية والدولية العالمية المعاصرة .

لقد اتّبع الكاتب في كتابة دراسته هذه أسلوبًا علميًا شيّقًا يُسهّل على القارئ العادي والمتخصص فهم الموضوع واستيعابه بكلّ سهولة ويسر، إذ استعرض مجموعة من المعلومات العلمية حول نوعية التقنيات التكنولوجية الحديثة وحجمها في ميدان الحرب الإلكترونية، وأهم الأدوات العسكرية المستخدَمة في الحرب الإلكترونية، مع عرض نماذج تطبيقية لتلك الاستخدامات. وتناول أيضًا مفهوم حرب الفضاء الإلكتروني من حيث الجوانب المتعلقة بأمن المعلومات الإلكترونية والقرصنة الإلكترونية، وكذلك الاستخبارات ومصادرها المفتوحة.

وعالج الكاتب مفهوم الحرب النفسية الإلكترونية وأدواتها، ومواقع التواصل الاجتماعي والحملات الإلكترونية المُستخدَمة فيها، كما وظف كافة المعلومات المتاحة في هذا المجال للإجابة عن التساؤل المحوري والأساسي الذي انطلق منه وهو: ما مدى التأثير الذي أحدثته التقنيات التكنولوجية الحديثة في تزايد الصراعات الدولية المعاصرة؟

وإضافة إلى ما سبق، يتميّز هذا الكتاب بمعلوماته العلمية الرصينة المستَمَدّة من مصادر ومراجع متخصصة وحديثة، فهو يُعَدّ من الدراسات العربية القليلة التي تناولت هذا الموضوع بالبحث والمعالجة، ولذلك يشكّل إضافة نوعية إلى المكتبة العربية، علمًا بأنّ موضوع هذه الدراسة منتشر بكثرة في الدراسات الغربية التي قامت بها مؤسسات بحثية ترتبط - بشكل أو بآخر - بالمؤسسات الرسمية في بلادها، مما يُفقِدها

الكثير من الحيادية، وخصوصًا عندما يتعلق الأمر بالصراعات في منطقة الشرق الأوسط، حيث يقلل كثير من تلك الدراسات من فرضية الاستخدام الواسع للتقنيات التكنولوجية في إدارة وتوجيه الصراعات في المنطقة العربية خصوصًا والعالم الثالث عمومًا.

ومن هنا، يُعَدّ هذا الكتاب إضافة علمية فريدة، حاول الباحث من خلاله أن يرصد بعيون علمية عربية أمينة الاستخدامات اللاإنسانية العديدة للتقنيات التكنولوجية الحديثة في الحروب والصراعات والنزاعات التي شهدتها المنطقة العربية والعالم .

ومن ثَمّ يقدم الباحث في نهاية دراسته دعوة لصانعي القرار ومتخذيه في الأنظمة والحكومات العربية إلى ضرورة الإلمام بالحدّ الأدنى من تلك التقنيات التكنولوجية، وفتح مراكز أبحاث ودراسات، وإنشاء تخصصات مستقلة في المعاهد والجامعات للاستفادة منها، بما يعود بالنفع والفائدة على العالم العربي.

أهنّئ الكاتب وأثَمّن له عاليًا المنهجية والموضوعية والنظرة النقدية التي اتّبعها والتزم بها، والتي مكنته في نهاية دراسته من الوصول إلى مجموعة من النتائج والتوصيات العلمية الرصينة، وهي جديرة بالبحث والتقصي لتكون مدخلًا إلى دراسات أخرى عديدة في هذا الميدان.

019/12/252

مقدمة

أحدثت التطورات الفكرية والصناعية التي وصل إليها الإنسان ثورة كبيرة في وسائل القتال والصراعات البشرية، فقد دخلت وسائل الاتصال الإلكتروني ساحة الصراعات البشرية لتحدث ثورة معلوماتية ضخمة في القطاعات الأمنية والعسكرية والسياسية، وهو ما أدى إلى تغيرات كثيرة في مفهوم الصراعات الحديثة، فبعد أن كانت الجيوش الجرارة والحشود العسكرية والقذائف القتالية هي لغة الصراع والقوة بين البشر أرضًا وجوًا وبحرًا، دخلت وسائل الاتصال الإلكتروني ساحة الصراع الإنساني لتضيف بعدًا جديدًا من أبعاد الصراع البشري، وهي حرب الفضاء الإلكتروني أو ما يعرف بالحرب الإلكترونية (Electronic Warfare).

فمنذ الحرب الروسية - اليابانية في عامي 1904-1905، ومرورًا بالحربين العالميتين الأولى والثانية، حتى يومنا هذا، أصبحت الحرب الإلكترونية في حالة دائمة التطور، ولم يعد خوض الاشتباكات الواسعة النطاق في العديد من الصراعات يتم في خنادق أرضية من قبل أعداد هائلة من المقاتلين، فالخطوط الأمامية في الحرب غالبًا ما يكون من الصعب تعريفها ما لم يُنظَر إليها من منظور الأنظمة الإلكترونية التي تسيطر على القوات، وتحدد مواقع الأهداف وهويتها، وتصوب الصواريخ بعيدة المدى، أو تنسق الضربات الجوية. واليوم يُعَدّ عنصر الحرب الإلكترونية

في المعارك الحديثة بالغ الحيوية للمفهوم الكلي للحرب، حتى إنّ نسبة كبرى من الأنشطة المعادية تتم في عالم فضاء المعركة غير المرئي، وهو منفصل وإن كان حاسمًا بالنسبة إلى مسرح العمليات التقليدي.

ومن ناحية أخرى، تحولت المواجهات في الصراعات المعاصرة من ساحة المعركة التقليدية إلى الوسائط الإعلامية والنصوص الإلكترونية، بهدف التعويض عن القدرات المادية، والتقليل من الخسائر البشرية، فأحدثت هذه الصراعات في ظل انتشار الإنترنت والبث الفضائي تأثيرات كبيرة جدًا في المجتمعات، وحققت أهدافًا استراتيجية لهذا النوع من الصراعات والحروب أوسع مما خُطِّط لها، فأصبحت المواجهات في الفضاء الإلكتروني تتعامل مع جميع المفردات المعلوماتية التي يتلقاها الكائن البشري بوصفه مجموعة أو أفرادًا أو كيانًا اجتماعيًا، بهدف إحداث التأثير من خلال التخويف والتهويل والتضليل المعلوماتي الذي يصور الخيال أقرب إلى الواقع، فنشطت هذه الأنواع من الحروب مؤخرًا.

لقد أصبح العالم يعتمد أكثر فأكثر على الفضاء الإلكتروني، ولا سيّما في البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية، إضافة إلى المؤسسات والشركات العامة والخاصة. ولا شكّ أنّ ازدياد الهجمات الإلكترونية التي نشهدها اليوم يرتبط أيضًا بازدياد هذا الاعتماد على شبكات الكمبيوتر والإنترنت في البنية التحتية الوطنية الأساسية، وهو ما

يعني إمكانية تطوّر الهجمات الإلكترونية اليوم لتصبح سلاحًا حاسمًا في النزاعات بين الدول في المستقبل.

ويستمر اليوم تطوير أساليب الحرب الإلكترونية وتقنياتها دون هوادة، وتتطور هذه الأدوات واستعمالاتها باستمرار للتصدي لأحدث التهديدات والتحديات، في دورة لا نهاية لها من الإجراءات المضادة للوسائل المستخدمة في الحرب الإلكترونية، هذا في ظل أعداد الهجمات الإلكترونية المتزايدة التي تتم في العالم اليوم، والتي تقوم بها مجموعات أو حكومات تتدرج في الاستهداف من أبسط المستويات إلى أكثرها تعقيدًا وخطورة. ويمكن اعتبارها وسائل تقنية حاسمة في الكثير من الصراعات المعاصرة التي تم الاستعاضة بها عن خوض الهجمات العسكرية والحروب التقليدية.

إنّ إدارة الحرب الإلكترونية بمهارة تفضي في النهاية إلى الحصول على معلومات تساعد في تدمير الأهداف بسرعة ودون إضاعة جهد، وتسمح للقادة بالسرعة في اتخاذ قرارات صحيحة، كما تتيح إمكانية التصدي لاستراتيجيات العدو بشكل سريع، وتحقيق النصر دون خسائر معوقة في الأرواح. إلّا أنّ إطار الحرب الإلكترونية لا ينحصر في استهداف المواقع العسكرية فقط، فهناك جهود متزايدة لاستهداف البنى التحتية المدنية والحسّاسة في البلدان المستهدَفة، وهو أمر أصبح واقعيًا في ظل القدرة على استهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام

المالي والمنشآت النفطية أو المائية أو الصناعية الحسّاسة بواسطة فيروسات على شبكة الإنترنت، بما يمكنها من إحداث أضرار مادّية حقيقية تؤدي إلى انفجارات أو دمار هائل.

يمكن اعتبار هذا الكتاب محاولة لتكوين صورة واضحة عن أعمال الحرب الإلكترونية التي أصبحت تحتل مكانًا بارزًا بين الأنشطة العسكرية المتعددة، وأصبح الشرق والغرب يولي الكثير من الاهتمام لتطوير وسائلها وأساليب استخدامها من جهة، وتسليط الضوء على دورها في الصراعات المعاصرة من جهة أخرى، بالإضافة إلى الاستخدام الكثيف لتكنولوجيا المعلومات وارتباطها الوثيق بمفهوم الحرب، حيث أصبح الفضاء الإلكتروني فاعلًا ومؤثرًا في النظام الدولي والعلاقات الدولية، وأصبحت المصالح الاستراتيجية ذات الطبيعة الإلكترونية عرضة للتهديد بتحول ساحة الصراع والحروب الدولية إلى الفضاء الإلكتروني، الأمرالذي جعل قضية أمن الفضاء الإلكتروني تلقى اهتمامًا متصاعدًا على أجندة الأمن الدولي.

وقد امتدّ هذا الاهتمام من حماية الدولة من التعرض لهجوم عسكري، إلى حماية المنشآت الحيوية للبنية التحتية من التعرض لأعمال هجومية باستخدام محكم لتكنولوجيا الاتصال والمعلومات، وتحليل الأثر الكبير للحرب الإلكترونية في نتائج الصراعات المعاصرة، وتسليط الضوء على أبرز التحولات في التقنيات العسكرية، وأحدث الأدوات التكنولوجية

لحرب الفضاء الإلكتروني، والاستخدامات الحديثة للإنترنت في مجال الحرب النفسية والوسائل الدعائية، وتأثير ذلك كلّه على الصراعات الدولية، وكيفية تأثيرها على إرادة الأطراف السياسية وقدرتها على عملية صنع القرار، ولا سيّما بعد الارتفاع الكبير في مستويات التقدم التكنولوجي والتقني والإلكتروني الذي أدى بدوره إلى جعل الفضاء الإلكتروني لأي دولة في العالم مستهدفًا، نظرًا للمكانة التي بات يحتلّها هذا الفضاء بين دول العالم، حيث بدت الخطورة التي أضحى الفضاء الإلكتروني يشكلها في إرادة الأطراف السياسية، وفي قدرتها على عملية صنع القرار، وهو المسرح الحقيقي الذي تتنازع الأطراف المتحاربة على استغلاله لمصلحتها. فإذا كان لا بدّ من ربط البنى التحتية الاستراتيجية بالإنترنت فإنه يجب تطوير الوسائل التقنية والإجراءات الإلكترونية الفعالة لحمايتها والدفاع عنها، وإدراك أهمية البرامج والأدوات الإلكترونية التي يتيحها الفضاء الإلكتروني للتأثير في الإرادة السياسية للفاعلين في النظام الدولي.

إنّ التقدم في العلوم التقنية والتكنولوجية يجعل وسائل الحروب أكثر دقّة، كما يجعلها تسبب خسائر أكبر، لذلك خلّفت الحرب الإلكترونية العديد من الآثار على الصراعات الدولية المعاصرة، وجعلت لأمن المعلومات الإلكترونية أهمية كبيرة في الدفاع عن مصالح الدول وبقائها.

وعليه فإنّ مسار تطور تكنولوجيا الصراعات الدولية المعاصرة يستند إلى الفرضيات التالية:

1. إنّ التطورات العديدة التي شهدتها القطاعات العسكرية والحربية جعلت منها مجالات ذات اعتمادية كبيرة على عنصري المعلوماتية والرقمية، وحولتها إلى أبنية تتسلح بأجيال جديدة من الأسلحة التكنولوجية والاتصالية، الأمر الذي زاد من قدراتها وفاعليتها في إدارة الصراعات ومواجهة التهديدات والتحديات.
2. كلّما زادت القدرة على القيام بهجمات إلكترونية - باستخدام الأدوات والوسائل التكنولوجية المتطورة التي يوفرها الفضاء الإلكتروني - ازدادت أدوات السيطرة والنفوذ الاستراتيجية في أوقات السلم والحرب، وذلك بسبب زيادة علاقة الفضاء الإلكتروني بعمل المنشآت الحيوية للدول المدنية منها والعسكرية، مما يؤدي إلى إمكانية تعرضها لهجمات إلكترونية تستهدف الشبكة كوسيط وحامل للخدمات، أو تشلّ عمل أنظمتها المعلوماتية، وهو ما يعرقل قدرتها على القيام بوظائفها.
3. يُعتبَر استخدام المعطيات الإلكترونية النفسية الوسيلة الأكثر فاعلية لإيجاد القناعات والآراء والاتجاهات التي تُسهِّل تأمين المصالح، وتعين على إدارة الصراع وتحليله.

الفصل الأول

مفاهيم ونظريات متعلقة بتكنولوجيا الصراعات الدولية

• المفاهيم

1. الحرب الإلكترونية

تعتبر المجالات العسكرية من البيئات المتجانسة والملتصقة بالحروب الإلكترونية. وتُعرّف الحروب الإلكترونية في هذا السياق بأنها مجموعة الأدوات والوسائل التقنية والرقمية التي تتسلح بها القطاعات العسكرية التي شهدت تطورات عديدة جعلتها تعتمد بشكل مباشر على عنصر المعلوماتية والرقمية، وحولتها إلى أبنية تتسلح بأجيال جديدة من الأسلحة التكنولوجية والاتصالية، وزادت من قدرتها وفاعليتها على الدعم اللوجستي والتواصل المعلوماتي والاستخباراتي القائم على توفر عنصر التقنية الحديثة، ممّا أضفى على الوسائل والأدوات العسكرية والحربية قدرًا كبيرًا من الدقة والجاهزية (بورجيلي، 2005: 12).

وتُعرّف الحرب الإلكترونية في هذا السياق أيضًا بأنها الحروب التي تتم بالتعاون مع الحروب العسكرية، إذ تصوب نيرانها نحو الأهداف الإلكترونية والرقمية والمعلوماتية، كالتجسس على الإشارات الصادرة عن الأجهزة الحاسوبية التابعة للفئات المستهدَفة، وبالتالي تستهدف هذه النيران الإلكترونية المصالح القومية والسياسية والعسكرية والأمنية للفئة المستهدَفة، متخذة لذلك شكل الهجمات الإلكترونية، أو الاختراقات الإلكترونية الهادفة إلى تعطيل البنية المعلوماتية لها (بدران، 2010: 30).

إلّا أنّ هناك من يربط مفهوم الحرب الإلكترونية ببيئة الإنترنت فقط، لأنها ساعدت على انتشار المعلومات في مختلف أنحاء المعمورة بشكل كثيف، وسهلت الوصول إليها بشكل سريع، بحيث يتم تعريف الحرب الإلكترونية بناء على ذلك بأنها: الحرب التي تستهدف المعلومات، وهي تعبير عن الاعتداءات التي تطال مواقع البيانات الموجودة على الإنترنت، وتحاول الاستيلاء على معطياتها، بين أطراف متناقضة الأهداف، ومتعارضة المصالح، ومختلفة المواقف (جاسم، 2010: 65).

ويُنظَر إلى الحرب الإلكترونية من الناحية النفسية والدعائية على أنها حرب العصر الحقيقية. ومسارها الرئيس هو الشبكات الرقمية والإلكترونية، وكذلك الوسائل والأدوات التكنولوجية الأخرى، والأدوات الإعلامية، وكلّ ما يتعلق بعالم المعلوماتية والحداثة. والغاية الرئيسية لهذه الحرب هي الأضرار النفسية والمعنوية بالدرجة الأولى، ثم تتبعها الأضرار المادية. وهي حرب ناعمة وصامتة ومظلمة، بعيدة عن الوسائل الحربية الخشنة، لكنها لا تمانع في امتطاء الترسانات المسلحة والعسكرية الضخمة (اليحياوي، 2010: 4).

2. الفضاء الإلكتروني

هناك من يرى أنّ هذا الفضاء ذو طابع افتراضي، حيث يتمّ تعريفه بأنه تلك البيئة الافتراضية التي تعمل فيها المعلومات الإلكترونية، والتي تتصل عن طريق شبكات الكمبيوتر. ويُعرّفها آخرون بأنّها المجال الذي

يتميز باستخدام الإلكترونيات لتخزين وتعديل وتغيير البيانات عن طريق النظم المرتبطة والمتصلة بالبيئة التحتية الطبيعية، ومن ثَمّ فإنه يشمل عملية الاندماج ما بين الإنترنت والمحمول وأجهزة الاتصالات والأقمار الصناعية (عبد الصادق، 2012: 28).

يمكن - بالتالي - اعتبار الفضاء الإلكتروني مجموعة من شبكات الحاسوب في العالم، وكلّ ما ترتبط به هذه الشبكات وتتحكم به. ويشمل هذا الفضاء الإنترنت إلى جانب العديد من شبكات الحاسوب السريّة الأخرى التي لا يمكن الوصول إليها عبر الإنترنت، وبعض هذه الشبكات الخاصة تشبه شبكة الإنترنت تمامًا لكنّها منفصلة عنها- على الأقل- نظريًا. كما يشمل الفضاء الإلكتروني الشبكات التجارية التي تقوم بمهام معيّنة من قبيل إرسال البيانات الخاصّة بالتدفقات المالية والمعاملات في الأسواق الماليّة ومعاملات البطاقات الائتمانيّة. وبعض الشبكات هي نفسها نظام للتحكم، بمعنى أنّها هي التي تسمح للأجهزة بمخاطبة غيرها من الأجهزة مثل لوحات التحكم التي تخاطب البنى التحتية الاستراتيجية كالمضخات ومولدات الطاقة والكهرباء (كلارك، 2012: 93).

3. أمن المعلومات الإلكترونية

هو العلم الذي يبحث في نظريات واستراتيجيات ووسائل حماية المعلومات الإلكترونية من المخاطر والأخطار التي تهدّدها، واتخاذ

الإجراءات والأدوات التكنولوجية لحماية تلك المعلومات من أية أنشطة اعتدائيّة ضارة قد تؤثر على فحواها وجوهرها (إبراهيم، 2008: 28).

4. حرب المعلومات

يرتبط مفهوم حرب المعلومات باستخدام المعلومات أو الهجوم على المعلومات كشكل من أشكال الحرب، ويمكن تعريفها: أيّ فعل أو نشاط يستهدف حرمان العدوّ من معلوماته أو استغلالها أو إفسادها أو تدميرها هي ووظائفها، وفي الوقت نفسه حماية النفس من هذه الأنشطة والأفعال (غيطاس، 2007: 6).

5. القرصنة الإلكترونية

يشير مفهوم القرصنة الإلكترونية إلى استخدام وسائل الاتصال وتكنولوجيا المعلومات الحديثة في ممارسات غير مشروعة، تستهدف التحايل على أنظمة المعالجة الآلية للبيانات، لكشف البيانات الحساسة (المُصنَّفة) أو تغييرها والتأثير على سلامتها أو حتى إتلافها. وبعبارة أخرى: ليست القرصنة سوى عملية دخول غير مصرَّح به إلى أجهزة الآخرين وشبكاتهم الإلكترونية، أي أنْ تُوجَّه هجمات إلى معلومات الكمبيوتر وخدماته، بقصد المساس بالسريّة أو المساس بسلامة المحتوى، أو تعطيل قدرة وكفاءة الأنظمة للقيام بأعمالها، فهدف هذا النمط الإجرامي هو نظام الكمبيوتر، وبشكل خاص المعلومات المخزَّنة

داخله. فالقرصنة تعني - إذًا - الوصول إلى أجهزة الآخرين بطريقة غير مشروعة من خلال ثغرات نظام الحماية الخاصّ بالهدف (محمود، 2005: 147).

6. استخبارات المصادر المفتوحة

هي عمليات الاستخبارات التي تستخدم المصادر المفتوحة من المصادر غير المحظورة. وهي كغيرها من أنواع الاستخبارات، لا تتوقف عند جمع المعلومات، بل تشمل تحليل المتطلبات وتصفية المعلومات وتحليلها، وتكاملها بعد جمعها. ويهدف هذا النوع من المعلومات إلى المساعدة في الحصول على إجابات مهمة لهدف ما، وقد يتم جمع معلومات حسّاسة من مصادر متعددة غير محظورة، ويتم دمجها لتشكل وحدة متكاملة، أو قد يتم استنساخ معلومات هامة من المعلومات المُجمَّعة من المصادر العامة (البداينة، 2002: 218).

7. الهندسة الاجتماعية

يُعنَى مفهوم الهندسة الاجتماعية باكتساب المعلومات الحسّاسة، أو ميزات الوصول غير المناسبة، من خلال إقامة علاقة ثقة غير ملائمة مع مستخدمي الشبكة العنكبوتية، وهي فنّ انتقاء الأفراد ليفعلوا أشياء ما كانوا ليفعلوها في الوضع الطبيعي. والهدف من هذا هو خداع شخص ما لتقديم معلومات قيّمة، أو الوصول إلى المعلومات. ويتمّ التركيز هنا على

الطبيعة البشرية مثل الرغبة في المساعدة، أو الرغبة في الثقة بالآخرين، أوالخوف من الوقوع في المشاكل (Tims، 2001: 1).

وقد ظهر مفهوم الهندسة الاجتماعية (Social Engineering) بوصفه فرعًا من فروع التكنولوجيا الناعمة (Soft Technology)، وامتدادًا طبيعيًا لعلوم الإعلام والاتصال نحو مجال الذكاء الاقتصادي أو التنافسي، فهي مزيج معقد من العلوم وعلم النفس والفنّ، ونستطيع تعريفها بأنّها:

«أيّ فعل يؤثّر في شخص كي يقوم بعمل أو يتخذ إجراء لا يكون بالضرورة في صالحه، مثل الإفضاء بمعلومات سريّة أو التصويت لصالح مرشح في انتخابات). وهي - بصفة عامة - مجموعة من الأساليب والتقنيات ذات منهج ترابطي يستند إلى التأثير (Influence) والخداع والنّصب والاحتيال (Super Cherie) والتلاعب (Manipulation) للحصول على معلومات شخصية سرية أو الوصول إلى نظام معلومات. ومن أقرب التعريفات لمفهوم الهندسة الاجتماعية أنّها استخدام المهاجم لحيل نفسية كي يخدع مستخدمي الحاسوب ليُمَكّنوه من الوصول إلى أجهزة الحاسوب أو المعلومات المُخزَّنة فيه» (أحمد، 2014: 22).

8. مواقع التواصل الاجتماعي

يشير مفهوم مواقع التواصل الاجتماعي إلى الطرق الجديدة للاتصال في البيئة الرقمية، بما يسمح للمجموعات الصغرى من الناس بإمكانية

الالتقاء والتجمع على الإنترنت وتبادل المنافع والمعلومات. وهي بيئة تسمح للأفراد والمجموعات بإسماع أصواتهم وأصوات مجتمعاتهم للعالم أجمع. ويمكن تعريف مواقع التواصل الاجتماعي أيضًا بأنّها منظومة من الشبكات الإلكترونية التي تسمح للمشترك فيها بإنشاء موقع خاصّ به، ومن ثم ربطه عن طريق نظام اجتماعي إلكتروني مع أعضاء آخرين لديهم الاهتمامات والهوايات نفسها.

9. الحملات الإلكترونية

هي عمل فردي أو شبه فردي يتحول إلى عمل جماعي «تطوعي» منظم يستهدف إحداث التغيير الاجتماعي والثقافي والسياسي داخل المجتمع، عن طريق استخدام الفضاء الإلكتروني كوسيط لحجم التفاعلات أو المزج بينه وبين فاعليات على أرض الواقع، وقد تكون الحملة مجرَّد ردّ فعل سرعان ما ينتهي، وقد تتحول الحملة إلى حركة من خلال قدرتها على الاستمرار، وما ترتبط به من قضية ذات أبعاد مختلفة، وكذلك حجم التأييد من جانب المجتمع ومؤسساته المعنية (عبد الصادق، 2013: 1).

• النظريات

يرتبط موضوع تكنولوجيا الصراعات الدولية بنظريتين أساسيتين، وهما نظرية الصراع ونظرية القوة الناعمة:

أولًا- نظرية الصراع

تتميز ظاهرة الصراع الدولي عن باقي ظواهر العلاقات الدولية بالتعقيد بسبب تعدد أبعادها وتداخل مسبباتها ومصادرها، وتشابك تفاعلاتها وتأثيراتها المباشرة وغير المباشرة. ومن الأمور التي يجدر التذكير بها عدم الخلط بين بعض المفاهيم المرتبطة بظاهرة الصراع كمسألة التفريق بين الصراع والحرب، فالصراع هو تصادم بين الإرادات الوطنية والتنازع الناتج من اختلاف الدول في الواقع والتصورات والأهداف والتطلعات، وهو ما يؤدي إلى اتخاذ قرارات وانتهاج سياسات خارجية تختلف أكثر مما تتفق.

فالصراع يشير في بعده السياسي إلى موقف تنافسي خاص، يكون طرفاه أو أطرافه على دراية بعدم التوافق في المواقف المستقبلية المحتملة التي يكون كلٌّ منهما أو منهم، مضطرًا فيها إلى تبني أو اتخاذ موقف لا يتوافق مع المصالح المحتملة للطرف الثاني أو الأطراف الأخرى. وبينما يهتم عالم الاجتماع الأمريكي «لويس كوزر» بالتركيز على الصراع في بعده الاجتماعي، تتجه عالمة الأنثروبولوجيا الأمريكية «لورا نادر» إلى إيضاح البعد الأنثروبولوجي* في العملية الصراعية. ومن ثَمّ فإنّ الصراع

---

* الأنثروبولوجيا: علم الإنسان والحضارات والمجتمعات البشريّة، وسلوكيّات الإنسان وأعماله، وقد ظهر مصطلح الأنثروبولوجيا الاجتماعيّة التي تُعنى بعلوم الإنسان ككائنٍ جماعي.

في بعده الاجتماعي إنّما يمثل «نضالًا حول قيم، أو مطالب، أو أوضاع معينة، أو قوة، أو حول موارد محدودة أو نادرة». ويكون الهدف هنا متمثلًا «ليس فقط في كسب القيم المرغوبة، بل أيضًا في تحييد، أو إلحاق الضرر، أو إزالة المنافسين أو التخلص منهم» (بدوي، 1997: 36).

إنّ الصراع في مثل هذه المواقف، كما يحدد «كوزر»، يمكن أن يحدث بين الأفراد، أو بين الجماعات، أو بين الأفراد والجماعات، أو داخل الجماعة أو الجماعات ذاتها. ويُرجِع كوزر تفسير ذلك إلى حقيقة أنّ الصراع في حدّ ذاته هو أحد السمات الأساسية لجوانب الحياة الاجتماعية. أمّا فيما يتعلق بالبعد الأنثروبولوجي للصراع، فإنّ الصراع ينشأ أو يحدث نتيجة للتنافس بين طرفين على الأقل، وقد يكون هذا الطرف متمثلًا في فرد، أو أسرة، أو ذريّة أو نسل بشري معيّن، أو مجتمع كامل. وإضافة إلى ذلك، قد يكون طرف الصراع طبقة اجتماعية، أو أفكارًا، أو منظمة سياسية، أو قبيلة، أو دينًا (Laura، 1968: 236).

ويرتبط الصراع هنا بالرغبات أو الأهداف غير المتوافقة التي تتميز بقدر من الاستمرارية والديمومة يجعلها تتميز عن المنازعات الناتجة عن الشطط، أو الغضب، أو التي تنشأ نتيجة لمسببات وقتية أو لحظية. وفي هذا الاتجاه يذهب قاموس لونجمان إلى تعريف مفهوم الصراع بأنّه «حالة من الاختلاف أو عدم الاتفاق بين جماعات، أو مبادئ، أو أفكار متعارضة، أو متناقضة». أمّا قاموس الكتاب العالمي فيُعرّف الصراع بأنّه

«معركة أو قتال Fight، أو نضال أو كفاح Struggle، وخصوصًا إذا كان الصراع طويلًا أو ممتدًا» (بدوي، 1997: 37).

وبوجه عام، فإنّ مفهوم الصراع في الأدبيات السياسية المتخصصة يُنظَر إليه «باعتباره ظاهرة ديناميكية»، فالمفهوم، من جانب، يقترح «موقفًا تنافسيًا معينًا، يكون كلٌّ من المتفاعلين فيه عالِمًا بعدم التوافق في المواقف المستقبلية المحتملة، كما يكون كلٌّ منهم مضطرًا أيضًا لاتخاذ موقف غير متوافق مع المصالح المدرَكة للطرف الآخر».

ومن هنا كان هناك اتجاه ينصرف إلى التركيز على البعد التنافسي في تعريف الصراع بأنّه «أحد أشكال السلوك التنافسي بين الأفراد أو الجماعات»، وأنّه «عادة ما يحدث عندما يتنافس فردان أو طرفان أو أكثر حول أهداف غير متوافقة، سواء كانت تلك الأهداف حقيقية أو مُتصوَّرَة، أو حول الموارد المحدودة». وفي تعريف آخر، يتميّز مفهوم الصراع بالبساطة والمباشرة، حيث يوصَف الصراع بأنّه «عملية منافسة ظاهرة، أو محتملة بين أطرافه». وهنا تثار أهمية التمييز بين الصراع وبعض أنواع المنافسة، كتلك التي تحدث في المجالات الرياضية على سبيل المثال، ففي المنافسة يتعاون الأفراد أو يتنافسون من أجل المرح وقضاء وقت طيّب وممتع، بينما في الصراع «يُعَدّ إحداث أو إلحاق الضرر المادي أو المعنوي بالآخرين هدفًا محددًا للصراع نفسه».

أمّا متغير «الإرادة» عند أطراف الصراع، فإنّه يمثل أساسًا محوريًا في تعريف الصراع لدى اتجاه آخر من كُتّاب الأدبيات السياسية، ومن ثمّ يتم

النظر إلى مفهوم الصراع باعتبار أنّه «في جوهره «تنازع للإرادات»، ينتج عن اختلاف في دوافع أطرافه، وفي تصوراتهم، وأهدافهم وتطلعاتهم، ومواردهم وإمكاناتهم، مما يؤدي بهم إلى اتخاذ قرارات، أو انتهاج سياسات تختلف فيما بينها أكثر ممّا تتّفق»، ومع ذلك، يظل الصراع دون نقطة الحرب المسلَّحة (المشاط، 1995: 4).

وهناك إضافة إلى ذلك، رأي ثالث يفضل الاهتمام ببنية الموقف الصراعي والمصالح المتضمنة فيه. ويمثّل مفهوم الصراع في هذا الاتجاه أو يعكس «موقفًا يكون لطرفين فيه أو أكثر أهداف أو قيم أو مصالح غير متوافقة إلى درجة تجعل قرار أحد الأطراف بصدد هذا الموقف سيئًا للغاية». ومن هنا يمكن النظر إلى مفهوم الصراع باعتباره «نتيجة لعدم التوافق في البنى والمصالح، مما يؤدي إلى استجابات بديلة للمشكلات السياسية الرئيسية». وعلى ذلك يخلص الكاتبان إلى «أنّ الصراع بهذه الكيفية، يُعَدّ سمة مشتركة لكلّ النظم السياسية الداخلية والدولية».

أمّا الصراع في مفهوم كوزر فإنّه يتبلور في ضوء القيم والأهداف التي تمثل الإطار المرجعي لأطراف الموقف الصراعي، وعلى ذلك يرى كوزر أنّ الصراع يتحدد في «النضال المرتبط بالقيم والمطالبة بتحقيق الوضعيات النادرة والمميزة، القوة والموارد، حيث تكون أهداف الفرقاء هي تحييد أو إيذاء أو القضاء على الخصوم، إضافة إلى أنّ هناك رؤى أخرى تسعى إلى توجيه الاهتمام نحو الأبعاد النفسية المتعلقة بعلاقات القبول والرفض بين أطراف الموقف الصراعي». ومن هنا تتجه تلك

الرؤى إلى تعريف الصراع فيها بأنه «ذلك العداء المتبادل بين الأفراد والجماعات أو الشعوب أو الدول على مختلف المستويات» (المشاط، 1995: 5).

وعلى ضوء ما سبق من نماذج التعريفات التي تقدمها أدبيّات الصراع بصدد التعريف وأبعاده المختلفة، يمكن الانتهاء إلى التأكيد على الأبعاد الثلاثة التالية كمحاور أساسية في التعريف بمفهوم الصراع (بدوي، 1997: 42):

1. **المحور الأول**: ويتعلق بالموقف الصراعي ذاته، ويشير إلى أنّ مفهوم الصراع يعبر عن موقف له سماته أو شروطه المحددة، فهو يفترض بدايةً تناقض المصالح أو القيم بين طرفين أو أكثر، وهو – ثانيًا – يشترط إدراك أطراف الموقف ووعيها بهذا التناقض، ثم هو يتطلب – ثالثًا – توافر أو تحقق الرغبة من جانب طرف (أو الأطراف) في تبني موقف لا يتفق بالضرورة مع رغبات الطرف الآخر أو (الأطراف الأخرى)، بل إنّ هذا الموقف قد يتصادم مع باقي هذه المواقف.
2. **أما المحور الثاني**: الذي يختص بأطراف الموقف الصراعي بوجه عام، فيمكن التمييز في الموقف الصراعي من حيث أطرافه بين مستويات ثلاثة: المستوى الأول يتعلق بالصراعات الفردية، أي التي يكون أطراف الصراع فيها أفرادًا، ومن ثَمّ فإن دائرة مثل هذا الصراع وموضوعه يتجهان إلى أن يكونا محدودين بطبيعتهما. وفي المستوى الثاني يكون الصراع بين جماعات، وتتعدد أنواع هذا الصراع بتنوع

أطرافه، كما أنّ دائرته ومجالاته تكون عادة أكثر اتساعًا وتنوعًا من نظيرتها في دائرة الصراع الفردي. أما المستوى الثالث فإنّه يختص بالصراع بين الدول الذي يُعرَف أيضًا بالصراع الدولي، وتكون دائرة (أو دوائر) الصراع فيه أكثر تعقيدًا واتساعًا من المستويين السابقين من الصراعات.

3. **المحور الثالث:** ويهتم بالصراع الدولي، وهنا تجدر الإشارة إلى أنّ اتساع دائرة المستوى الثالث من الصراعات - عبر المراحل التاريخية المتعاقبة للعلاقات الدولية - كان من شأنه توجيه وتكتيل قدر متزايد لا يستهان به من الجهود العلمية والأكاديمية لدراسة وتأصيل الظاهرة الصراعية، بهدف تطوير التفسيرات والنظريات العلمية التي تُيسِّر فهم أسبابه ومحدداته، ومن ثَمّ تقدم البدائل المختلفة التي يمكن من خلالها التحكم في الظاهرة الصراعية، أو على الأقل التقليل من المخاطر المرتبطة بها والمترتبة عليها، وتحديد أساليب التعامل معها. وقد أسفرت الجهود العلمية في هذا المجال عن تراث غني وأصيل من النظريات والتفسيرات، ولعلّ من بينها نظريات المعرفة العقلانية، والنظرية السُّلالية، ونظريات القوة، ونظريات صنع القرار، والاتصالات، والنظم، وغيرها من النظريات المُفسِّرة للصراع في أبعاده المختلفة: النفسية والبيولوجية والثقافية والاجتماعية والاقتصادية والسياسية، ومؤخرًا البيئية والحضارية..

إنّ المحور الثاني هو الأكثر ارتباطًا بهذه الدراسة، حيث أدّت الحرب الإلكترونية إلى بروز دور الأفراد والجماعات كفاعلين مؤثرين في النظام الدولي. وقد تغير منظور الصراع جذريًا، حيث انتقلت من نسق «الصراعات بين الدول إلى وسط الشعوب»، فكان الغرض من الحرب قديمًا هو تدمير الخصم، إمّا باحتلال أرضه، أو الاستيلاء على موارده. أمّا الحروب الجديدة، فقد استهدفت بالأساس التحكم في إرادة المجتمعات وخياراتها، ومن ثَمّ، احتلّت الشّعوب أهمية محورية في هذا النمط الجديد من الحروب، سواء تعلق الأمر بالسكان المُستهدَفين في أرض المواجهة، أو بالرأي العام في الدولة التي تشن الحرب، أو بالرأي العام على الصعيدين الإقليمي والدولي.

سباق التسلح

يخلق إطار السرّية المرتبط بسباق التسلح مناخًا من الشكّ والخوف وعدم اليقين لدى الأطراف المعنية، الأمر الذي لا يساعدها على حلّ المنازعات السياسية، بل قد يكون سببًا في الدفع نحو الصدام والصراع. ويدفع استمرار التطور التكنولوجي في مجالات ونظم التسلح بدوره مجموعات المصالح المرتبطة به نحو مواصلة ضغوطها على دوائر صنع القرار للإبقاء على كلّ أو بعض بؤر التوتر والصراعات ساخنة وملتهبة، بما يضمن مصالح هذه الجماعات بأقصى درجة ممكنة.

وتتمثل أهم الانتقادات الموجهة إلى هذا المدخل في أنّ سباق التسلح - في حدّ ذاته- لا يمكن أن يكون بمفرده سببًا في خلق الصراع الدولي، فهو -وإن أدى إلى زيادة التوتر وشحن أجواء الصراعات - لا ينتج بذاته صراعًا، فالصراع سوف يستمر، حتى في ظل إمكانية التوصل إلى إجراءات نزع السلاح، وذلك لأنّ جذور الصراع ما زالت قائمة دون حلّ، ومن ثَمّ يصبح المطلوب هو تصفية أو تسوية هذه الجذور، مما يبرر إضعاف اللجوء إلى سباق التسلح.

لقد شهدت القطاعات العسكرية والحربية تطورات عديدة جعلت منها مجالات ذات اعتمادية كبيرة على عنصري المعلوماتية والرقمية، وحولتها إلى أبنية تسلح بأجيال جديدة من الاسلحة التكنولوجية والاتصالية، وزادت من قدراتها وفاعليتها على الدعم اللوجستي، والتواصل المعلوماتي والاستخباراتي القائم على توفر عنصر التقنية الحديثة الذي أضفى على الوسائل والأدوات العسكرية والحربية قدرًا كبيرًا من الدقة والجاهزية (بو رجيلي، 2005: 11).

فالثورة التكنولوجية في ميدان الأسلحة، وما تؤدي إليه من حدوث فجوة في نظم التسلح بين الدول المتقدمة وما دونها، يدفع الأولى إلى المبادرة بشنّ الحرب قبل أن تفقد الدولة مزايا التطور التكنولوجي الذي تمتلكه في مواجهة الأطراف الأخرى. إنّ التفوق التكنولوجي في نظم التسلح يدفع أيضًا إلى استعراض القوة كوسيلة للضغط بصدد التسوية

الدبلوماسية، مما يؤدي إلى شحن الصراعات بمزيد من التوتر والعنف بصرف النظر عن الأسلوب المقصود أو غير المقصود الذي قد يحدث (بهاز، 2010: 45).

وقد ظهر نوع من الصراعات الدولية هو صراع المعلومات الّذي يحدث عندما تفتقد الأطراف المعلومات الضرورية اللازمة لاتخاذ القرارات الحكيمة، أو عندما يتم تزويدها بمعلومات غير صحيحة، أو عندما تختلف هذه الأطراف حول أهمية المعلومات، أو تختلف في تفسيرها، أو عندما يصل الأفراد إلى تقييمات مختلفة بصورة جذرية لنفس المعلومات (بدوي، 1997: 58).

ويجب الإشارة هنا إلى أنّ حدوث صراعات المعلومات قد لا يكون ضروريًا، لأنها تقع نتيجة سوء الاتصالات أو انعدامها بين أطراف الصراع، كما أنّ بعض صراعات المعلومات قد تكون صراعات حقيقية وقوية، لأنّ المعلومات أو الإجراءات التي استخدمها الأفراد في جمعها، قد تكون غير متوافقة، أو قد يكون كلٌّ من المعلومات والإجراءات مفتقرًا إلى التوافق.

ثانيًا- القوة الناعمة

ظهر مؤخرًا نوعان من متغيرات القوة، هما: انتقال القوة، وانتشار القوة. ويُعدّ انتقال القوة من دولة مهيمنة إلى دولة أخرى واقعة تاريخية مألوفة، أمّا انتشار القوة فهو عملية أكثر جدة، وتتمثل مشكلة كافة الدول

في عصر المعلومات العولمي الحالي في أنّ أكثر الأشياء تحدث خارج نطاق سيطرة الدول حتى أقواها.

يُعَدّ مفهوم القوة أحد المفاهيم المركزية في العلاقات الدولية منذ القدم بالرغم من تطوره من فترة زمنية إلى أخرى، وفقًا للسياق المحيط والعوامل الدولية المؤثرة في طبيعته. وتُعرَّف القوة بأنها القدرة على تحقيق الأهداف والنتائج المرجوة، ويُعرِّفها روبرت داهال (Dahl) بأنها القدرة على جعل الآخرين يفعلون ما لم ينووا القيام به. ويقف (ناي) عند هذا التعريف ويشير إلى أنّه إذا أردنا إدراك مفهوم القوة وقياسه وفقا لهذا التعريف، فإننا بحاجة إلى معرفة تفضيلات الآخرين، وكذلك سلوكهم إذا لم تمارس عليهم القوة، وهو ما لا يمكن التوصل إليه في حقيقة الأمر. ومن هذا المنطلق اعتبر القادة السياسيون أنّ مثل هذا التعريف غير عملي، وأصبح التعريف التقليدي للقوة هو امتلاك المصادر التي تشمل السكان والأرض والموارد الطبيعية، وحجم الاقتصاد، والقوات العسكرية، والاستقرار السياسي. فهذا التعريف بالنسبة لهم واقعي ومحدَّد، ويمكن به قياس القوة وتحديدها، ولكن أصبحت الجدلية هي أنّ المصادر تكون أولى بالاستخدام وفقًا للظروف والسياق والمواقف التي تُستخدَم فيها (Joseph، 1990: 177).

وتبرز هنا مشكلة أساسية هي عملية تحويل القوة (power conversion) كما أشار إليها (ناي)، وتعني كيفية تحويل المصادر إلى قوة فعلية، وقدرة

الفواعل الدولية على ذلك، إذ يرتبط التفوق في القوة بالقدرة على تحويل هذه الموارد وليس امتلاكها فقط، وبذلك أصبح مُحدِّد القوة هو امتلاك الموارد والقدرة على تحويلها إلى قوة فعلية. وتجدر الإشارة إلى أنه مع تطور التكنولوجيا الصناعية وبالتالي تغير طبيعة القوة العسكرية - ولا سيّما في الحروب - أصبحت القوة النووية مصدرًا جديدًا للقوة يتسم بالأهمية، ولكنّه سرعان ما تلاشى عندما أصبح استخدامها غير منطقي، ولا تلجأ الدول إليه في حروبها.

فمفهوم القوة الصلبة يشير إلى المفهوم التقليدي للقوة الذي يُعَرّف القوة بأنّها القدرة على فرض السيطرة على الآخرين عن طريق الإكراه أو الحوافز المادية. وتُعتَبر المصادر الأساسية للقوة الصلبة هي القوة العسكرية والقوة الاقتصادية، وعليه يمكن ممارسة القوة وفقًا لناي باتباع طريقة من ثلاث: إمّا بتهديدات الإكراه (العصا) أو التحفيز (الجزرة) أو عن طريق (الجذب)، فالطريقتان الأولى والثانية يصنفان تحت مصطلح القوة الصلبة، والأخيرة هي القوة الناعمة (ناي، 2015: 19).

يشير مفهوم القوة بشكل عام إلى القدرة على فرض السيطرة على الآخرين وجعلهم يفعلون ما لا يريدونه. وترتبط القدرة على السيطرة بامتلاك موارد معينة تتناول بشكل عام السكان والأرض والموارد الطبيعية وحجم الاقتصاد والقوات المسلحة والاستقرار السياسي. ولعلّ الاختبار التقليدي للقوة كان يتمثل في قدرتها على تحقيق الانتصار في

الحروب، ولكنّ هذا المفهوم تغير اليوم بشكل كبير، ولم يَعُد يركز على القوة العسكرية والقدرة على الغزو والاحتلال، كما كان في الفترات السابقة، فقد انتقل التركيز إلى مصادر القوة الحديثة كالتكنولوجيا والتعليم والنمو الاقتصادي التي اعتُبِرت جوهرية في تقدير القوة الدولية (أبو ليلة، 2012: 5).

يشير مفهوم القوة الناعمة كما عرَّفه (ناي) إلى أنه اتّجاه أكثر جاذبية لفرض القوة يختلف عن الوسائل التقليدية، فالدولة تستطيع تحقيق الأهداف التي تسعى إليها في السياسة الدولية لأنّ غيرها من الدول ترغب في أن تتبعها، أو لأنها ارتضت وضعًا معينًا يصنع مجموعة من النتائج المترتبة تستهدفها الدولة التي تمارس قوتها، وهذا يحدث عندما تستطيع الدولة جعل غيرها من الدول يرغب فيما ترغبه هي. وترتبط القدرة على التأثير في الآخرين وتوجيه رغباتهم وتحديدها بمصادر معنوية أو غير مادية للقوة كالثقافة والأيديولوجية والمؤسسات (Joseph، 1990: 189).

وتُعرَف القوة الناعمة كذلك بالـ «Co-optive power» التي تعني قدرة الدولة على خلق وضع يفرض على الدول الأخرى أن تحدد تفضيلاتها ومصالحها بشكل يتفق مع هذا الإطار الذي تم وضعه، أو – بمعنى آخر – أن تقوم هي بوضع أولويات الأجندة الداخلية لغيرها من الدول. وأكد (ناي) كذلك على عنصر الجاذبية الذي تعتمد عليه القوة الناعمة، فالقوة الناعمة تعني لديه القدرة على تحقيق أهداف معينة عن

طريق الترغيب والجاذبية لا الترهيب والإكراه. وتعتمد القوة الناعمة على عنصرين أساسيين هما المصداقية والشرعية كقاعدة لها (عبد الصبور، 2013: 51).

كما حدّد «جوزيف ناي» ثلاثة مصادر رئيسية للقوة الناعمة، تتمثل في:

- القيم السياسية للدولة حين يتم تطبيقها بمصداقية داخل الدولة وخارجها.
- القيم السياسية للدولة عندما يراها الآخرون مشروعة.
- ثقافة الدولة عندما تكون جاذبة للآخرين.

ويشير ناي إلى بعدين لتلك الثقافة، تُعبّر عن البعد الأول الثقافة النخبوية التي تتمثل في التعليم والفنّ والأدب، وتُعبّر عن البعد الثاني الثقافة الشعبية.

وتعتمد الدراسة على مفهومي القوة الناعمة والقوة الذكية في تحليل الأدوات المستخدمة في الحرب الإلكترونية، فالهجمات الإلكترونية تُحدِث أضرارًا جسيمة يمكن أن تسببها الدولة في الصراع الإلكتروني لدولة أخرى، دون الحاجة للدخول المادي إلى أراضيها، وذلك لأنّ تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية جعل هذه الأخيرة عرضة للهجوم المزدوج.

مفهوم القوة الذكية في العلاقات الدولية:

قدّم جوزيف ناي مبتكِر مفهوم القوة الناعمة مفهوم القوة الذكية عام 2003 كردّ فعل على المغالطة بشأن الفكرة السائدة بأنّ القوة الناعمة يمكن أن تعمل وحدها لتحقيق أهداف السياسة الخارجية، وضرورة الانتقال إلى المعنى الأوسع والأشمل للاستراتيجية وتطويرها لتشمل القوة الناعمة والقوة الصلبة معًا، وذلك ليكون أكثر مواكبة للسياق والتطورات الدولية المختلفة بحيث لا يمكن الاستغناء عن أيٍّ من نوعي القوة.

لم يعد الفصل بين القوة الناعمة والقوة الصلبة مقبولًا في السياق الدولي الحالي، علاوة على ظهور الفواعل غير الدولية التي استطاعت أن تدمج بين القوتين الناعمة والصلبة. كما أنّ عصر العولمة أصبح يفرض قيودًا على طبيعة استخدام القوة، والاستراتيجية التي يجب اتباعها لتحقيق المصالح والأهداف المنشودة في السياسة الدولية.

ويعود ذلك إلى تغير طبيعة النظام الدولي وقضاياه وموضوعاته، وإلى تغير طبيعة السكان والشعوب والحاجة إلى استهدافهم بما يتناسب مع هذا التغير. كما أصبحت كثافة المعلومات وسرعتها تخلق مناخًا مختلفًا من العلاقات الدولية، بحيث باتت المعلومات هي القوة، فمن يملكها ويوظفها يكون قادرًا على أن يفرض سيطرته. وقد ظهر لنا ما عُرِف

بحرب الشبكات والحروب الإلكترونية كنتيجة لذلك (عبد الصادق، 2009: 31).

ويمكن القول بأنّ هناك تحولًا كبيرًا قد حدث للدول الثمانية العظمى، تَمثّل في تحول اقتصادها من اقتصاد صناعي إلى اقتصاد ما بعد صناعي، أي أنّها أصبحت تعتمد في قوتها على قدرة الدولة على خلق وتسخير المعرفة والمعلومات لزيادة قوتها. فقدرة الدول على الإبداع والابتكار قد تزيد من قوة الدولة بما يفوق ما قد تحققه زيادة القوات المسلحة. فعلى الرغم من أنّ القوة العسكرية ما زالت لها أهميتها، تغيرت أهميتها النسبية من حيث كيفية استخدامها ودمجها مع الأصول غير العسكرية، فهناك نقلة نوعية وتغير في طبيعة التأثير بين دول العالم (Emest، 2008: 114).

إنّ مفهوم القوة الذكية ليس مفهومًا جديدًا أو مبتكَرًا، بل هو نتاج الجمع بين القوة الصلبة والقوة الناعمة معًا وفقًا لاستراتيجية محدَّدة تجمع بينهما. ويُعَرّف أرنست ويلسون القوة الذكية بأنّها قدرة الفاعل الدولي على مزج عناصر القوة الصلبة والقوة الناعمة بطريقة تضمن تدعيم تحقيق أهداف الفاعل الدولي بكفاءة وفعالية. ويحدد هذا التعريف مجموعة من الشروط الإضافية التي يجب توافرها لتحقيق القوة الذكية (ناي، 2015: 242) وهي:

1. الهدف من ممارسة القوة، فالقوة لا يمكن أن تكون ذكية دون أن يعرف ممارسوها الهدف من استخدامها، والشعوب والمناطق المستهدَفة من هذه القوة.
2. الإدراك والفهم الذاتي للأهداف بالاتساق مع القدرات و الإمكانيات المتاحة، فلا يمكن للقوة الذكية أن تعتمد على الأهداف دون تحديد عنصري الإرادة والقدرة على تحقيقها.
3. السياق الإقليمي والدولي الذي سيتم في نطاقه تحقيق الأهداف.
4. الأدوات التي سيتم استخدامها، بالإضافة إلى وقت وكيفية توظيفها منفصلة أو مع غيرها.

فالفاعل بحاجة إلى إدراك مخزون الدولة من الأدوات والإمكانات ونقاط القوة ونقاط الضعف والقيود على مقدرات القوة، والقوة الذكية ليست فقط امتلاك المصادر الناعمة والصلبة والمزج بينها، بل القدرة على تحديد وقت استخدامها، وتحديد نوع القوة الّذي يفضل استخدامه حسب الموقف، والقدرة على تحديد متى يتم الدمج بينهما، وكيف يتم هذا الدمج. فالاتجاه المركّب لتفسير القوة من خلال القوة الذكية يعني التعامل مع عناصر القوة الناعمة والصلبة، ليس على أساس كونهما منفصلتين، بل على التعامل مع عناصرهذين النوعين من القوة ككلّ، والتعامل مع التداخل القائم بينهما. (عبد الصبور، 2013: 49).

الفصل الثاني

الثورة في تقنيات الحرب
وتطبيقاتها في الصراعات الدولية

زادت الاستراتيجيات العسكرية الجديدة والثورة في الشؤون العسكرية من قدرة قادة الجيوش على تقرير مجرى الحرب وقيادتها وهم جالسون في مقر قياداتهم أمام شاشات تلفزيونية وحاسوبية كبيرة، تنقل لهم صورًا عن أهداف العدو الاستراتيجية التي يمكنهم توجيه ضربات مدمرة لها بمجرد النقر على مفاتيح تُطلِق الصواريخ المُوجَّهة والقادرة على إصابة أهدافها بدقة بالغة، كما يمكنهم تعطيل أجهزة اتصالات العدو وراداراته بواسطة أشعة الليزر المنطلقة من الأقمار الصناعية.

وقد شهدت القطاعات العسكرية والحربية تطورات عديدة جعلت منها مجالات تعتمد بشكل كبير على عنصر المعلوماتية والرقمية، وحولتها إلى أبنية تسلح بأجيال جديدة من الأسلحة التكنولوجية والاتصالية، وزادت من قدراتها وفاعليتها على الدعم اللوجستي والتواصل المعلوماتي والاستخباراتي القائم على توفر عنصر التقنية الحديثة، ممّا أكسب الوسائل والأدوات العسكرية والحربية قدرًا كبيرًا من الدقة والجاهزية. وهذه التطورات الكبيرة في التقنيات الحديثة التي طرأت على الأسلحة المستخدمة في الحرب هي نتاج عدد من الابتكارات (hundley، 2010: 15) أهمها:

1. التكنولوجيا الحديثة التي أدت إلى ظهور الأجهزة والأنظمة التي كانت مستحيلة سابقًا أو غير مفكر فيها.
2. الأجهزة الجديدة التي اعتمدت على التكنولوجيا الحديثة.
3. الأنظمة الحديثة التي تعتمد على الأجهزة الحديثة.

4. المفهوم الجديد للعمليات.

5. العقيدة الجديدة وهيكلة القوات.

وبتوجيه النظر تاريخيًا نحو تطور التقنيات العسكرية المُستخدَمة في الحرب، نجد أنّ روسيا قد طوّرت في العهد السوفييتي استراتيجية سمتها القتال الإلكتروني اللاسلكي، وهي تُعرِّفها بأنها الجمع بين الحرب الإلكترونية وأسلحة التدمير المادي لحرمان العدو من السيطرة الإلكترونية على قواته. ويُعَدّ القتال الإلكتروني جزءًا لا يتجزأ من خطة الحرب الروسية، ففي حال حدوث حرب مع حلف الناتو مثلًا، سوف تتمثل استراتيجية روسيا في تدمير ما أمكن من قوات الناتو بالمدفعية والهجمات الجوية قبل المعركة الرئيسية، وفي الوقت نفسه يتم استهداف عناصر مختارة من أنظمة القيادة والسيطرة التابعة للناتو بالقتال الإلكتروني اللاسلكي، بحيث تُترَك في حالة ارتباك وتُحيَّد بصورة فعالة، وإذا نجحت هذه الخطة فإنّ بقية قوات الناتو تصبح ضعيفة إلى حدّ يمكن فيه التغلب عليها بسرعة.

وفي المقابل تمّ تصميم الاستراتيجية الأمريكية المكافئة التي تُدعى الإجراءات المضادة للقيادة والسيطرة والاتصال (C3CM) في ثمانينيات القرن الماضي، وتعرف هذه الإجراءات بأنها الاستخدام المتكامل لأمن العمليات والخداع العسكري والتشويش والتدمير المادي بمساندة الاستخبارات، ويتمثل هدفها في التأثير في المعلومات وإضعاف قيمتها أو تدميرها، وفي حرمان قدرات العدو على القيادة والسيطرة والاتصالات

الصديقة من إجراءات مماثلة، وتُعدّ الحرب الإلكترونية عنصرًا من هذه الاستراتيجية، حيث تتمثل وظيفتها في السيطرة على الطيف الكهرطيسي، لأنّ للأسلحة والطائرات المقاتلة والاستخبارات والاتصالات والأنظمة العسكرية الأخرى مهام محددة ضمن هذه الاستراتيجية (Quinn،Portar، 2001 : 14).

ويمكن حصر العوامل التي أدت إلى هذا التطور في طبيعة وسلوك العمليات العسكرية في النقاط التالية (أولمان، بي ويد، 2000: 83):

1. تبلور مفهوم جديد للحرب يختص بحرب المعلومات (information warfare).
2. تبلور تكتيك جديد للقتال يُسمَّى القتال المُتمركِز على الشبكات (network-centric warfare).
3. تَشكُّل وحدات القيادة والسيطرة المتكاملة.

(Integrated Command and Control)

لقد كان كافيًا في الماضي الحديث عن القيادة والسيطرة (command and control) عند الإشارة التي يتلقى بها الضباط المسؤولون المعلومات من مرؤوسيهم عن أوضاع المعركة، ومن ثَمّ يصدرون الأوامر بشأن ما ينبغي فعله بعد ذلك. وفي وقت لاحق أصبح من الممكن والمرغوب به في آن واحد إبقاء القوات على اتصال في مسارح العمليات، في الوقت الذي تتوارد فيه المعلومات الاستخباراتية من أنظمة متخصصة، وليس فقط من الوحدات التي كانت في تماسّ مباشر مع العدو، وقد أدى ذلك إلى دراسة

جوانب القيادة والسيطرة والاتصالات والاستخبارات (command, control, communications and intelligence) (C3I) باعتبارها تشكل مجموعة متماسكة من المشكلات. ويتناول محللو الدفاع الآن جوانب القيادة والسيطرة والاتصالات واستخدام الحواسيب والاستخبارات وإدارة المعركة وفقًا للطريقة نفسها. وعلى الرغم من أنّ المصطلح المختصر (C4I/BM) أي القيادة والسيطرة والاتصالات واستخدام الحواسيب والاستخبارات وإدارة المعركة (command, control, communications, computers, intelligence and battle management) يختزل كلّ هذه العناصر في عبارة واحدة تقريبًا، فإنه يوحي بأنّ نظم المعلومات غدت أمرًا ضروريًا لنطاق واسع وشامل من الواجبات والمهام، وبأنها تُعتمَد أيضًا بالمعنى الدقيق بصورة متبادلة مع بعضها البعض (فريدمان، 2000: 14).

وفي تسعينيات القرن الماضي أثمرت محاولات دراسات تأثير الانتقال إلى عصر المعلوماتية على الأمن تطورًا في مفهوم الثورة في الشؤون العسكرية، وخرجت هذه الفكرة من رحم الابتكارات التكنولوجية الحديثة التي رفعت مستوى نوعية المعلومات الاستخباراتية وحداثتها، وزادت في تطور التقنيات العسكرية ودقة الوسائل القتالية. وحدثت خلال الأعوام التي تلت - وبصورة خاصة في بدايات القرن الحادي والعشرين - تطورات تكنولوجية متقدمة في مجال الحرب الإلكترونية، أدّت إلى تغييرات نوعية في خصائص ميدان القتال، وكذلك في أنماط قتال الجيوش الحديثة، مما أدى إلى التأثير في الصراعات

الدولية المعاصرة بشكل كبير. وسيتم في هذا الفصل التركيز على تقنيات الحروب الإلكترونية وأسلحتها مع نماذج تطبيقية لاستخداماتها في الصراعات الدولية، وذلك ضمن مبحثين مستقلين.

• الأدوات العسكرية في الحرب الإلكترونية

قامت معظم الدول المتقدمة عسكريًا في السنوات الأخيرة بالتركيز على مجالين أساسيين في تكنولوجيا معدات الحرب الإلكترونية:

المجال الأول: الإعاقة الإلكترونية وإسكات معدّات العدو الإلكترونية، ويذهب هذا المجال إلى أبعد من ذلك ليشمل السيطرة الإلكترونية المباشرة على معدات العدو، و**المجال الثاني**: هو تطوير وبدء استخدام الإنسان الآلي (Robots)، وكذلك الطائرات دون طيار. وستساعد هذه التطبيقات كثيرًا على تخفيف أعداد الضحايا من الجنود، كما أنها ستعزز العمليات الخاصة في التجسس وكشف المجهول، فالمستقبل هو حتمًا للتكنولوجيا الحربية وأسلحتها، ولم يعد ممكنًا بأيّ حال الاعتماد على الأسلحة التقليدية مهما كان عددها أو قوة تدميرها. أمّا الدول التي لا تستطيع المنافسة والابتكار فستخسر ثقلها العسكري وبالتالي وزنها السياسي.

ومن هنا فإنّ التطور الكبير في الأدوات العسكرية والتقنيات المستخدمة فيها يعتمد على التفاعل بين النظم التي تجمع المعلومات

وتعالجها وتدمجها وتنقلها، والنظم التي تستخدم القوة العسكرية. وسوف يعمل ما يسمى (نظام النظم) على جعل هذا التفاعل سلسًا ومستمرًا قدر الإمكان. ونتيجة لذلك سيتم توجيه القوة العسكرية بطريقة حاسمة ومدمرة ضد عدوّ ما يزال منهمكًا في عملية تعبئة الموارد ووضع الخطط، حيث تطرح هذه الرؤية تحقيق نصر سريع وكامل في الصراعات الدولية بحد أدنى من المخاطر.

يمكن تكوين أنظمة الحرب الإلكترونية (EW) لمجموعة متنوعة من المهام المختلفة، واستخدام مجموعة من الأنظمة الفرعية المختلفة. ولكن على الرغم من هذا التعقيد والتنوع المذهلين، تبقى هناك ثلاث قدرات رئيسية مشتركة لمعظم أنظمة الحرب الإلكترونية، وهي: استشعار البيئة (مستشعِر المستقبل)، وتحليل البيئة (تحليل الإشارة)، والاستجابة للبيئة (توليد التقنية ونقل الطاقة العالية).

الإحساس بالبيئة وفهمها: يجب أن يكون لنظام الحرب الإلكترونية - سواء تم تكوينه للهجوم أو الحماية أو الدعم - طريقة لجمع وفهم الإشارات في بيئته. ويجب تحديد ما هو موجود، وفهم كيفية استخدامه للطيف، وتحديد ما إذا كان يمثل تهديدًا. هذه هي قدرة «الاستقبال» للنظام، وعادةً ما يتم تنفيذها بواسطة نظام فرعي يسمى مستقبِل الإنذار بالرادار(Radar Warning Receiver).

معالجة التهديدات وجها لوجه: إذا اكتشف مستقبِل الإنذار بالرادار(RWR) إشارة، وحدّد التحليل أنّ هناك تهديدًا لا مفر منه، يجب على نظام الحرب الإلكترونية (EW) تحييده، ثم تمرير بيانات التهديد إلى مُوَلّد التقنية الذي يحدد كيفية استجابة النظام لمعالجة التهديد. سيختار منشئ التقنية تقنية تشويش ذات احتمالية أعلى للنجاح استنادًا إلى عدد من العوامل، بما في ذلك خصائص التهديد الخاص، ومنصة استضافة نظام الحرب الإلكترونية ومجال المعركة - برية أو بحرية أو جوية.

البث والإرسال: لكي يتمكن نظام الحرب الإلكترونية من تنفيذ هجمات إلكترونية أو مهمات حماية إلكترونية، يجب أن يكون قادرًا على بثّ إشارات خاصة به للسيطرة على الطيف الكهرومغناطيسي. وبمجرد تحليل التهديد وخلق استجابة، فإنّ قدرة مرسل (أجهزة) نظام (EW) على إشعاع الطاقة الكهرومغناطيسية بدقة تجعل التشويش والخداع وغيرهما من الإجراءات الإلكترونية المضادة ممكنة.

يعتبر استخدام تكنولوجيا الإلكترونيات في الأغراض العسكرية نقطة تحول كبيرة، سواء في فن الحرب أو في إدارة الصراع المسلح، فقد احتلّت أسلحة القتال الحديثة ومعداته مكان الصدارة في حسم أي صراع مسلح، وخاصة أسلحة الهجوم الجوي الحديثة لاعتمادها على نُظم السيطرة والتوجيه الإلكتروني التي تُمكِّنها من تنفيذ المهام المطلوبة منها

بكفاءة، وإصابة أهدافها بدقة عالية نظرًا لاستخدامها نُظم ووسائل الكشف والتوجيه والتحكم، وقيادة النيران وتصحيحها لاسلكيًا، وراداريًا، وحراريًا، وليزريًا، وتليفزيونيًا، وهي النُّظم التي يستوي تشغيلها واستخدامها ليلًا ونهارًا. هذا إضافة إلى النظم الحديثة والمتقدمة للتصوير التليفزيوني باستخدام آلات التصوير ذات الحساسية العالية، التي يمكنها العمل في مستوى الضوء المنخفض بكفاءة ودقة عاليتين.

وهناك العديد من الأدوات والوسائل التقنية والرقمية التي تتسلح بها الحرب الإلكترونية، وتحديدًا في القطاعات العسكرية التي شهدت تطورات عديدة جعلتها تعتمد بشكل مباشر على عنصري المعلوماتية والرقمية، وحولتها إلى أبنية تتسلح بأجيال جديدة من الأسلحة التكنولوجية والاتصالية، وزادت من قدرتها وفاعليتها على الدعم اللوجستي والتواصل المعلوماتي والاستخباراتي القائم على توفر عنصر التقنية الحديثة، وهو ما أضفى على الوسائل والأدوات العسكرية والحربية قدرًا كبيرًا من الدقة والجاهزية، وفيما يلي بعض من تلك الوسائل والأدوات العسكرية:

1. الأسلحة الروبوتية:

الروبوتات بشكل عام هي آلات تُبنى على ما يطلق عليه الباحثون نموذج «أَحسِسْ– فكِّرْ– تحرّكْ» أي أنها أجهزة من صنع الإنسان تحتوي على ثلاثة مكونات رئيسية (Finkelstein، 2016: 22) هي:

1. المِجسّات (sensors) التي ترصد البيئة وتكشف التغيرات فيها.
2. المعالِجات (processors) أو الذكاء الاصطناعي الذي يقرر كيفية الاستجابة.
3. المؤثرات (effectors) التي تؤثر في البيئة على نحو يعكس القرارات المُتّخَذة، بما يخلق نوعًا من التغيير في العالم المحيط بالروبوت.

يصنِّف غالبية المراقبين لساحات الحروب أجهزة الروبوت العسكرية في خانة آلات القتل والتدمير والتجسس ذات الطاقة المرعبة، حيث تمثل في الواقع الجندي المثالي، فهي لا تتعب ولا تكلّ ما دامت مصادر طاقتها تعمل، كما أنّ ردة الفعل لديها أسرع بكثير من الجنود البشريين، وهي تستطيع رفع ونقل ما يزن عدة أضعاف وزنها من الأثقال. وهذه السمات تجعل الروبوت متفوقًا من الناحية القتالية على العنصر البشري.

تُعرِّف الأمم المتحدة الروبوتات القاتلة المستقلة بمنظومات سلاح قادرة عند تشغيلها على اختيار أهداف معينة، والاشتباك معها دون الحاجة إلى تدخل إضافي من العنصر البشري. وهي آلات ومنظومات

تكنولوجية مصنوعة وفق النموذج الإدراكي القائم على الشعور والتفكير والفعل، وهي مُزوّدَة بأجهزة استشعار تسمح لها بقدر من الإدراك للظرف، ويمكنها بواسطة المعالجة أو الذكاء الاصطناعي تقرير الاستجابة لحافز مُعيّن والشروع في تنفيذ القرارات.

وقد ابتُكِرت روبوتات تستطيع تتبع تضاريس الأرض، واختيار طرق بديلة، ومنها ما يستطيع حمل الإمدادات من الأسلحة والذخيرة وتطهير الأرض من الألغام، والاضطلاع بأعمال الحراسة. وما زال العمل جاريًا على تطويرها، لتصبح قادرة على اللمس والشمّ والسمع والتذوق، وكلّ ما يُحسّن أداءها، ويزيدها سرعة ومقدرة في إنجاز مهماتها. كما تطمح الولايات المتحدة الأمريكية على وجه الخصوص إلى تطوير روبوت يحارب في الخطوط الأمامية، ويستطيع تسلق الحواجز، ويسبح تحت الماء، ويراقب الروبوتات العسكرية الأخرى، كما جنّدت روبوتًا كروي الشكل يتدحرج على الأرض، ويستقر على ثلاث قوائم تلسكوبية، ويخرج رأسه من فتحة فيه مستطلعًا المكان المحيط لاكتشاف قوات العدو، فتبادر مستشعرات الحرارة والحركة المُزوَّد بها إلى تجهيز أسلحة في داخله وتصويبها من خلال فتحة أخرى نحو الأعداء (علو، 2011: 96).

وقد اتخذ الجيش الأمريكي قرارًا باستخدام الجندي الروبوت الذي يحمل اسم «سووردز» (swords) في ميدان العمليات في العراق. ويتكون اسم هذا

الروبوت من الأحرف الأولى لـ«نظام الأسلحة الخاصة للمراقبة والاستطلاع» (special weapons observation reconnaissance detection system) ويُعَدّ هذا الروبوت الذي يبلغ طوله مترًا واحدًا أول سابقة في التاريخ العسكري في مجال العمليات البرية. ويعمل الجنود الذين يبلغ عددهم 18 وحدة بنظام التحكم عن بعد، وكلّ نظام مُجهَّز بأربع كاميرات تصوير، وفيه خاصية الرؤية الليلية وعدسات مُقرِّبة، وهو مزود بمسدس من نوع M240 أو M249، كما يمكنه السير على الصخور والجبال وتخطي الأسلاك الشائكة، ويعمل ببطاريات تكفي لتشغيله أربع ساعات، وفيه وحدة للتحكم عن بعد تحتوي على عَصَوين للتحكم وشاشة فيديو. وسيمثل هؤلاء الجنود الدفعة الأولى من العناصر الآلية التي يستعملها الجيش الأمريكي في معارك حقيقية. ويقول قادة الجيش الأمريكي إنّ الجندي الروبوت سريع الحركة، ويمكنه تقفي أثر الأعداء والهجوم عليهم، مقللًا بذلك المخاطر التي يتعرض لها الجنود الأمريكيون (JOSHUA، 2005: 5).

أما الروبوتات الطائرة (من دون طيار) فتقوم فكرتها في الأساس على مفهوم الروبوتات الطائرة لعمليات الاستطلاع، مع تطويرها بحيث يمكنها المشاركة في القتال وخوض المعارك الجوية، وقصف الأهداف الأرضية بكفاءة الطائرات القاذفة نفسها، فهي تمثل صورة أخرى من صور التقنية الحديثة في الحرب، حيث تُعَدّ مؤشرًا نحو الميل إلى

الاستغناء عن الطيارين في المهام القتالية الخطرة. وقد أكدت العمليات الحربية أهمية هذه الروبوتات في عملية الاستطلاع، مثل طائرة غلوبال هوك (global hawk) التي استخدمت بنجاح في حرب أفغانستان عام 2001، وطائرة بريديتور (predator) التي بدأ استخدامها في حرب البلقان وأفغانستان والعراق. وقد حظيت هاتان الطائرتان باهتمام القادة العسكريين لأنهما وفّرتا لهم صورًا حية بالفيديو عن أنشطة العدو على الأرض في وقت قياسي، كما وفّرتا فرصة تهديف وإطلاق صواريخ محملة عليهما، مما دفع الخبراء إلى تصميم أجيال من الطائرات المماثلة التي لا تكتفي بتنفيذ عمليات الاستطلاع فحسب، بل تهاجم المواقع المعادية أيضًا (سلامة، 2005: 24).

لقد غيّرت الطائرات دون طيار عوامل كثيرة في الحروب، مثل التكلفة البشرية والمادية، والزمان والمكان، وحتى مفهوم القوة، علاوة على أنها قدمت تسهيلات كبيرة لكلّ من يحوز هذه التقنية، ولعبت دورًا بارزًا ومتنوعًا في كثير من الحروب، وحفَّزت الدول على تصنيعها أو الحصول عليها.

2. حرب الدرونز:

الدرونز (الطائرات دون طيار) هي أسلوب حديث من حروب التحكم عن بعد، يمكن من خلالها الاستغناء ولو بشكل جزئي عن شنّ هجمات ضخمة على الأرض تهدد بشكل كبير حياة القوات البرية. وهناك عشرات

الأنواع المختلفة من الطائرات دون طيار، إلا أنها تنقسم بشكل عام إلى فئتين: تُستخدَم الأولى لأغراض الاستطلاع والمراقبة، وتكون الثانية مُسلّحة بالصواريخ والقنابل، وقد أصبحت الطائرات دون طيار أحدث سلاح مُفضَّل فيما يسمى الحرب على الإرهاب، إمّا للاستطلاع عن مواقع الإرهابيين ومخططاتهم، أو لتنفيذ هجمات ضدهم.

وفي الجانب الآخر أصبح الآن بإمكان الإرهابيين تأمين نفقات الطائرات دون طيار وبالتالي سهولة استخدامهم لها. ويمكن القول بأنّ هذه الطائرات دون طيار قد غيَّرت بالفعل مسار الحرب الحديثة، وستسمح هذه «الدرونز» للجهات الفاعلة من غير الدول بتشكيل تهديد خطير للدول ذات السيادة أو لقواتها المسلحة، وخصوصًا أنّ هذه الطائرات يتم تجهيزها بالكاميرات أو حتى بالمتفجرات، وهي قادرة على قطع الكيلومترات، ويمكن تركيبها بالفعل بأجزاء يتم طلبها من الإنترنت.

وتعود جذور فكرة الطائرات دون طيار تاريخيًا كجزء من الحرب إلى استخدام النمساويين بالونات الهواء الساخن دون طيار لقصف البندقية عام 1848م، وقد تقدمت تكنولوجيا الطائرة دون طيار في فترة ما بين الحربين العالميتين الأولى والثانية، وقد بدأ استخدام مصطلح الطائرة دون طيار في ذلك الوقت بعد أن طوّرت المملكة المتحدة «ملكة النحل»، وهي طائرة ثنائية تم تحويلها ليتم التحكم بها عن طريق الراديو من الأرض.

كانت طائرة (Queen Bee)- مثل العديد من الطائرات العسكرية دون طيار في ذلك الوقت - محركًا يتم التحكم فيه عن بُعد ليستخدمه المدفعيون المضادون للطائرات لتحديد الهدف. وبحلول أواخر الخمسينيات من القرن الماضي وجدت الولايات المتحدة ودول أخرى أنّ بإمكانها استخدام طائرات دون طيار موجهة عن بعد كطائرات تجسس. وحلقت الطائرات دون طيار التي يتم التحكم فيها عن طريق الراديو وكاميرات الأفلام فوق الصين وفيتنام الشمالية لجمع معلومات استخبارية، ولكن دون المخاطرة بحياة الطيارين.

كانت الطائرات المُسيّرة لا تزال مجرد تقنية متخصصة خلال الحرب الباردة، وكانت صغيرة وغير موثوقة إضافة إلى أنها باهظة الثمن، وكان على الطيارين أن يبقوا ضمن نطاق إشارات الراديو التناظرية الخاصة بهم، وغالبًا ما يضطرون إلى التحليق بطائراتهم دون طيار أثناء وجودهم في طائرة مأهولة قريبة.

أمّا الطائرات دون طيار الأمريكية فقد بدأت كطائرات تجسس وتطورت لتصبح أسلحة اغتيال، وقد تم استخدامها في سبع دول على الأقل لأداء هذه الأدوار، طوال حرب واشنطن المستمرة منذ 15 عامًا على الإرهاب، فقد كانت هذه الطائرات تجمع المعلومات، وتلبي حاجة الجيش التي لا تنضب للحصول على معلومات استخباراتية في ساحة المعركة، وكانت قادرة على إيجاد الإرهابيين والمتمردين وقتلهم.

توسعت حرب الطائرات الأمريكية دون طيار بشكل كبير في عهد الرئيس باراك أوباما، ردًا على التهديدات المتطرفة والتوافر الأكبر لتكنولوجيا الطيران عن بعد، ويُذكَر أنّ أوباما وجّه خلال فترة ولايته أوامر باستخدام الطائرات دون طيار لمكافحة الإرهاب أكثر بعشر مرات من سلفه جورج دبليو بوش.

ولم يقتصر الأمر على وضع الرئيس السّابق أوباما أكثر من نوع من الطائرات دون طيار في السماء، بل جعل توظيف الطبيعة المنخفضة لضربات الطائرات دون طيار من السهل - سياسيًا - على الولايات المتحدة أن تشنّ عمليات في بلدان لم تكن في حالة حرب معها من الناحية الفنية، ونَفذت وكالة المخابرات المركزية وقيادة العمليات الخاصة المشتركة في البنتاغون مئات الضربات في اليمن وباكستان والصومال..

وبالمجمل كان تأثير حرب الطائرات دون طيار على المدنيين الذين يعيشون في أفغانستان وباكستان - مثلًا - بالغ الخطورة، مع وقوع العديد من الضحايا المدنيين، والتهديد المستمر بشن هجمات من طائرات دون طيار تحلق في السماء لمدة تصل إلى 17 ساعة في المرة الواحدة. فعلى الرغم من الادّعاءات بأن الطائرات دون طيار هي «أسلحة دقيقة»، توضح التقارير حول عدد القتلى من غارات الطائرات دون طيار في باكستان واليمن والصومال أنّ ما بين 201–213 طفلًا قتلوا منذ عام 2001، وأنّ تقديرات الخسائر بين المدنيين تتراوح بين 2985 و 4533.

وبالإضافة إلى عدد القتلى، فإنّ الأثر النفسي للعيش تحت المراقبة المستمرة، وعدم معرفة متى ستحدث الضربة التالية هو اعتبار جدّي. وقد وجد الباحثون في جامعة ستانفورد وجامعة نيويورك في تقرير (Living Under Drones) أنّ المدنيين في باكستان «يتعرضون لترويع» الطائرات دون طيار.

والمثال الواقعي لاستخدام الإرهابيين للطائرات دون طيار يكمن في الهجوم الذي وقع بتاريخ 14/ 9/ 2019 ضدّ معملين لأرامكو في السعودية، حيث نُفِّذ باستخدام ما يصل إلى 19 طائرة درونز، وضرب المعتدون مصفاة نفط مهمة في بقيق وحقل نفط قرب خريص. وادَّعت ميليشيا الحوثيين مسؤوليتها عن ذلك الهجوم الذي كان له عواقب وخيمة على الاقتصاد العالمي، فيما أعلنت السعودية أنّ إيران زودت الحوثيين بطائرات من دون طيار، وحمَّلتها المسؤولية عن الهجوم الجوي في أرامكو. والنتيجة هنا ما خلَّفته تلك الهجمات من القلق، فما مدى ثقة المجتمع الدولي في قدرة الميليشيات على تنفيذ مثل هذه الهجمات الإرهابية؟ وبالتالي فإنّ الإرهابيين يمتلكون أيضًا طائرات مقاتلة، ولكنّها نماذج بدائية تمامًا، لا يمكن السيطرة عليها عن طريق الأقمار الصناعية واستخدامها في جميع أنحاء العالم، ولكنها ذات تأثير نفسي مقلق.

وقد أظهر الهجوم الذي شنته عدة طائرات دون طيار على منشآت النفط أنّه يمكن للمجموعات غير الحكومية الآن استخدام الطائرات التي يتم التحكم بها عن بُعد لشنّ هجمات واسعة النطاق. فحقيقة أنهم يستخدمون الآن طائرات دون طيار لتنفيذ هجوم سربي باتت تمثل نهجًا جديدًا في الاعتماد على هذه الطائرات.

ويمكن - إضافة إلى ذلك - شراء طائرات دون طيار تحمل حمولات كبيرة، وتتعامل مع مسافات أطول بشكل قانوني، فالتوافر التجاري لمثل هذه الطائرات ليس له عواقب على الأمن في المناطق المضطربة مثل الشرق الأوسط. يقول كريستيان مولينغ وتوربن شوتز من جمعية السياسة الخارجية الألمانية في ثينك تانك في مقابلة مع صحيفة فرانكفورتر الألمانية (FAZ) : «هناك عدد متزايد من الجهات الفاعلة قادرة على استخدام الصواريخ كسلاح»، «وبالإضافة إلى الأهداف العسكرية، فإن البنى التحتية المدنيَّة الهامة تقع في مرمى النار، وقد لا يتم اكتشاف المهاجمين».

ويبقى السؤال هنا: هل الأسلحة المستقلة أخلاقية في مجال الصراع؟ إنّ إدخال الذكاء الاصطناعي إلى الأسلحة العسكرية لا يناسب الجميع في النظام الدولي، وقد أدى هذا إلى إنشاء اللجنة الدولية لمراقبة الأسلحة الآلية (ICRAC) التي تقودها (Human Rights Watch)، وتقوم بحملة

متعددة الأطراف من أجل حظر استخدام أنظمة الأسلحة المستقلة الفتاكة (LAWS).

وتتمثل حُجّة اللجنة الدولية لمراقبة الأسلحة الآلية (ICRAC) في ثلاثة محاور:

أولًا - تقول المجموعة إنّ من المستحيل ضمان امتثال (LAWS) للقانون الإنساني الدولي، وخصوصًا عندما يتعلق الأمر بالتمييز بين المقاتلين والمدنيين.

ثانيًا - ليس لدى هذه الآلات قيود أخلاقية، نظرًا لعدم قدرتها على فهم ما يعنيه أن تكون في دولة القانون، ناهيك عن إنهاء حياة الإنسان.

ثالثًا - تخشى مجموعة (ICRAC) أن يكون لـ (LAWS) تأثير ضار على الأمن العالمي، وخصوصًا في حالة استخدامها من قبل جهات فاعلة غير مسؤولة عن الأطر القانونية التي تحكم استخدام القوة.

تقول لوسي سوشمان أستاذة الأنثروبولوجيا والعلوم والتكنولوجيا في جامعة لانكستر، والعضو في مجموعة اللجنة الدولية لمراقبة الأسلحة الآلية (ICRAC): «إنّ أنظمة الأسلحة المستقلة الفتاكة هي تلك التي يتم فيها تفويض المهام الحاسمة لاختيار الهدف، وبدء استخدام القوة العنيفة للنظام بطرق تمنع التحكم البشري الهادف، وإنّ موقف الحملة هو أنّ تصميم أنظمة الأسلحة يجب أن يجعلها غير قادرة على العمل دون

سيطرة بشرية ذات مغزى، وهذا من شأنه أن يجعل الأسلحة المستقلة الفتاكة غير قانونية».

وأخيرًا - بصرف النظر عمّا إذا كان الروبوت العسكري «غبيًا» أم «ذكيًا» - تبقى الأسئلة حول استخدام الذكاء الاصطناعي في بيئة عسكرية قائمة ومطروحة. ولا يوجد حتى الآن دليل يذكر على أنّ الأنظمة الحالية التي تدعم الذكاء الاصطناعي خالية تمامًا من الأخطاء، فعلى سبيل المثال، يستخدم المستهلكون أجهزة التعرف على الصوت مثل (Echo Amazon) و(Siri) بشكل خاطئ، أو يسيئون فهم الأوامر، لكنّ نتائج مثل هذه الأخطاء التي تحدث في المنزل لا يمكن مقارنتها بتلك التي قد تحدث في ساحة المعركة.

ومع صعود الحرب السيبرانية، تظهر أيضًا مخاوف بشأن ما قد يحدث في حالة اختراق روبوت عسكري، فهل من المعقول أنّ الروبوتات المصممة لتقليل عدد الجنود على الأرض - وبالتالي - الحدّ من الضحايا البشرية - يمكن أن يكون لها تأثير معاكس، وتزيد فقط من الصراع؟ فلا بدّ من معالجة هذه النقاط قبل اتخاذ خطوات لاحقة في مجال الروبوتات العسكرية.

3. الأسلحة الفضائية:

تلعب تكنولوجيا الفضاء دورًا حيويًّا في الحرب الحديثة، فقد شهدت السنوات الأخيرة اهتمامًا ملحوظًا بتكنولوجيا الأقمار الصناعية

العسكرية، واستخدامها في الاتصالات والتجسس والاستطلاع والإنذار المبكر بشكل دقيق وفي الوقت المناسب. وتزايدت أعداد الدول التي تسعى لامتلاك هذه الأقمار، وتنامت قدراتها، مما يؤكد الدور الحيوي للبعد الفضائي كأحد عناصر تحقيق التوازن الاستراتيجي، حيث يُذكَر أنّ الولايات المتحدة تمتلك ما يقرب من 110 أقمار صناعية لها صلة بالأغراض العسكرية، أمّا روسيا فلديها 40 قمرًا صناعيًا، بينما تمتلك بقية دول العالم مجتمعة 20 قمرًا صناعيًا فقط. وفي حرب الخليج الثانية عام 1991 أطلقت الولايات المتحدة الأمريكية نحو 40 قمرًا صناعيًا في منظومات ذات واجبات خاصة، تركزت مهمتها في الرصد والإنذار المبكر للتحركات الجوية العراقية، وخصوصًا الأسلحة الصاروخية، وتأمين الاستطلاع الفضائي (الصدّ والمراقبة والتصوير الإلكتروني)، ومراقبة الاتصالات العراقية والتشويش عليها، وجمع المعلومات الملاحية من الأحوال المناخية، وتأمين الاتصالات لقوات التحالف الدولي.

فرض الفضاء نفسه كبعد استراتيجي رابع في الصراعات المسلحة، وليس مجرد مجال لعبور السفن الفضائية أو الصواريخ الباليستية، فهو أساسًا مجال واسع يَمنح مَن يملك السيطرة عليه امتيازات كبيرة، تتمثل في جمع المعلومات باستخدام أجهزة المراقبة في الأقمار الصناعية والسفن الفضائية التي يُمكنها أن ترصد فعليًا كلّ ما يحدث في أيّ منطقة

من العالم، وكذلك معالجة المعلومات والسيطرة على وسائل الاتصال، وهو ما يجعل من البيانات شيئًا مفهومًا ومفيدًا، تعرضه على شاشة تحدد أهدافًا للصواريخ والمقذوفات، مثل: الأهداف الصغيرة كالدبابات، أوالتصرُّف وفقًا لأهمية وحجم المعلومات في شنّ الغارات الجويَّة بعيدة المدى وبالغة الدقة، لتدمير الأهداف بأقمار صناعية تَصِل دقتها إلى حدّ أن تنسف مجمعًا صغيرًا على بعد مئات الأميال.

4. الرادار:

يُعَدّ الرادار أحد أهم أجهزة الحرب الإلكترونية، فهو عين إلكترونية يمكنها أن ترى في الظلام أو الضباب وتخترق سُدَف الدخان، كما يمكنه الكشف عن اقتراب العدو إلى مسافات أكبر بكثير مما تراه العين المجردة، وتوجيه نيران المدفعية في أحوال الرؤية الضعيفة، وحتى التزويد بالمعلومات المتعلقة بالسمات الطبوغرافية لمنطقة ما (daniel، 1992: 5).

لم يكن الرادار أداة من أدوات الحرب الإلكترونية فقط، بل كان الهدف الأساسي منها الذي تسعى الجهة المعادية إلى تحديده، فجهاز الرادار يتألف عادة من مرسِل ومستقبِل وهوائي وشاشة (مبين راداري)، يقوم بإرسال مجموعات نبضات ذات قدرة كهرطيسية عن طريق هوائي ذي تشويش عالٍ يعمل ضمن اتجاه محدد، وعند اصطدام النبضات بهدف – كطائرة مثلًا خلال رحلتها – ترتدّ عائدة أو تنعكس باتجاه

المستقبِل. ويتم قياس الزمن الذي تستغرقه النبضات خلال ذهابها وارتداد صداها بواسطة أداة خاصة موجودة في جهاز الرادار، وبما أنّ سرعة الأمواج الكهرطيسية هي 300000 كم/ ث فإنّ مسألة حساب مسافة بُعد الهدف عن الرادار أصبحت سهلة جدًا، وأصبح بإمكان عامل الرادار قراءة مسافة الهدف واتجاهه على شاشة الرادار مباشرة (الأشرم، 1988: 53).

ويُعتبَر الرادار وسيلة مهمة في أعمال الرصد. ولأجل فهم ذلك علينا تعقّب عمله وفق التسلسل الآتي (خالد، 1990: 60):

1. تقوم مرسِلة جهاز الرادار ببثّ موجات لاسلكية متناهية القصر بشكل حزمة ضيقة عن طريق الهوائي.
2. تمسح هذه الحزمة قطاع الرصد المعين أفقيًا وعموديًا.
3. عند اصطدام الحزمة بجسم ما كطائرة أو صاروخ مثلًا، تنعكس على شكل صدى.
4. تستلم آخذة الرادار الصّدى عن طريق الهوائي نفسه، ويظهر على صورة نقطة مضيئة.
5. يُحدَّد مدى الهدف بحساب الزمن المستغرَق بين إرسال النبضة واستلامها، وفق حقيقة أنّ سرعة النبضة اللاسلكية هي 300000كم/ ث، والمسافة تساوي نصف حاصل ضرب سرعة النبضة في الزمن المستغرَق لاستلام النبضة.

6. تُحسَب سرعة الهدف عن طريق ملاحظة معدل التغيير في موقع الهدف على شاشة الرادار.
7. يُحدِّد اتجاه الهوائي عند التقاط الهدف سمتَ الهدف بالنسبة لموقعه.
8. تُحسَب زاوية النظر من الفرق بين المستوى الأفقي للشعاع وزاويته في لحظة اصطدامه بالهدف.
9. تُدخَل المعلومات المُحَصّلَة من (مسافة، سمة، وزاوية نظر) إلى حاسب إلكتروني، بعد تزويده بمعلومات مسبقة عن العوامل الجوية المؤثرة وخصائص حركة مقذوفات العدو، فيمكن بذلك معرفة الموقع الذي انطلق منه المقذوف واكتشافه.

• تقنية المستشعِرات القريبة والبعيدة المدى

المستشعِرات بعيدة المدى هي تلك المستشعِرات التي تُجَهَّز بها الأقمار الصناعية التي تدور حول الأرض في مدارات فضائية منخفضة ومتوسطة الارتفاع، وطائرات الاستطلاع التي تطير على ارتفاعات شاهقة، والطائرات المُوجَّهة دون طيار التي تنطلق من القطع البحرية، أو من طائرات حاملة خاصة، وتتميز هذه المستشعرات بالآتي (البصيلي، 1989: 64):

أ. تنوع تقنيات الاستشعار المستخدمة من القمر الصناعي أو الطائرة بحيث تشمل الاستشعار الضوئي، والحراري، والكهرومغناطيسي.

ب. زيادة المساحة التي يغطيها المستشعر في اللقطة الواحدة، مع قدرة التمييز العالية بين الأهداف المتقاربة.

جـ. المقدرة على إرسال المعلومات المُكتشَفة إلى مراكز التجميع والتحليل والدمج الأرضية في نفس لحظة اكتشافها.

د. صغر الحجم وانخفاض مستوى الطاقة اللازمة لعمل هذه المستشعرات، الأمر الذي يتيح استخدام أقمار صناعية أو طائرات أصغر حجمًا وأقل تكلفة.

هـ. إمكانية تصفية المعلومات والتعامل مع المعلومات ذات الأهمية العسكرية فقط، والتخلص من المعلومات غير المهمة، لتقليل حجم المعلومات المطلوب معالجتها وتبادلها عبر وسائل الاتصال.

أمّا المستشعِرات قصيرة المدى فهي تلك المستشعِرات التي تعمل من فوق منصات طائرة، أو من فوق منصات برية، أوعائمات بحرية، وهذا يؤدي إلى قصر مدى المراقبة مقابل زيادة المقدرة على التمييز، وتشمل هذه النوعية من المستشعِرات - بالإضافة إلى ما سبق ذكره - وسائل استشعار الاهتزازات مثل المستشعرات الصوتية والمغناطيسية (خليل، 2001: 23).

التقنية في الاتصالات العسكرية:

لا تختلف أجهزة معدات الاتصال العسكرية - من الناحية النظرية والتصميم ونظريات العمل - عن تلك المستخدمة في المجالات المدنية،

فمكونات جهاز الاتصال اللاسلكي الرئيسة واحدة، حيث يتكون بصفة عامة من وحدة إرسال، ووحدة استقبال، وتتكون كلٌّ منهما من الوحدات الفرعية الآتية (أحمد، 200: 12):

أ. **وحدة الإرسال:** وتتكون من محوِّل الصوت إلى إشارات كهربائية في الميكروفون، ووحدة تكبير التردد السمعي، ومعدِّل التردد، ومكبِّر القدرة، وهوائي الإرسال.

ب. **وحدة الاستقبال:** وتتكوّن من هوائي الاستقبال، ومكبِّر التردد العالي، ووحدة خفض التردد، ومكبِّر التردد البَيني، ووحدة الكاشف، ومكبِّر التردد السمعي، ووحدة البيان الصوتي، والسماعات.

ورغم اشتراك مُعدّات الاتصال العسكرية والمدنية في المكونات الرئيسة فإن هناك أوجه اختلاف جوهرية بينها، أهمها أسلوب التصنيع، فإنتاج الأجهزة الإلكترونية بصفة عامة، وأجهزة الاتصالات بصفة خاصة، يتم وفق مستويات معينة من المواصفات، تبدأ من المعدات ذات المواصفات التجارية وتنتهي بأعلى هذه المواصفات، وهي مواصفات المُعدّات العسكرية (Military Standards). والمعدات ذات المواصفات القياسية العسكرية هي التي تستطيع التغلب على الظروف الطبيعية القاسية في ميادين القتال، وكذلك ظروف المعارك الحربية، وما يمكن أن تتعرض له تلك المعدات من أحوال مختلفة. وتُعَدّ المعدات

ذات المواصفات القياسية العسكرية أعلى تكلفة من المعدات ذات المواصفات القياسية الأخرى (بورجيلي، 2005، 18).

تطبِّق الاتصالات العسكرية مبدًا مهمًا هو استخدام القدرة التي تكاد تكفي لتحقيق الاتصال الآمن، وذلك كي لا يستفيد العدو من استقبال الرسائل المتبادلة. ولذلك تتنوع قدرات أجهزة الإرسال المستخدَمة، كما تتنوع أيضًا تلك الأجهزة طبقًا لخواص انتشار الموجات الكهرومغناطيسية في الأوساط المختلفة، إذ تحتاج الاتصالات العسكرية إلى تحقيق الاتصال بين قوات تعمل على سطح الأرض (القوات البرية)، وبين الطائرات في الجو، وبين السفن في عرض البحر، وأحيانًا مع الغائصات (مكاوي، 1993: 53).

أدى تطور العلوم الإلكترونية، وظهور مكونات الدوائر الإلكترونية التي تعمل باستخدام الأساليب الرقمية، إلى إدخال الاتصالات العسكرية في حقبة جديدة أطلق عليها اسم حقبة تحول ميدان القتال إلى استخدام الأساليب الرقمية. ويتلخص أبرز ما حققه هذا التحول في مجال الاتصال بالآتي:

أ. تصغير حجم المُعدّات مع تخفيف وزنها إلى نسبة قد تصل أحيانًا إلى عُشر وزن المعدات التي لا تستخدم الأساليب الرقمية، وهذا يقلل من حجم مراكز الإشارة العسكرية والاتصالات الثابتة على مختلف المستويات، مما يقلل ظهورها وتعرضها لهجمات العدو،

كما يتيح إمكانية استخدام مراكز إشارة متحركة ومجهَّزة فوق مركبات برية أو قطع بحرية، وبعضها مجهّز على متن طائرات خاصة تؤدي دورًا رئيسًا في تحقيق الاتصالات العسكرية.

ب. زيادة سرعة الاتصالات وكفاءتها وسريتها، وإتاحة فرصة دمج العديد من الوظائف التي كان يحتاج تنفيذ كل منها مُعِدَّة مستقلة في مُعِدَّة واحدة.

ج. استخدام الكود بأنواعه ودرجاته المختلفة وكذلك الشّيفرة في الرسائل المتبادلة، بلغ درجة عالية من الرقي إلى حدّ أصبحت فيه نسبة كبيرة من الوثائق والرسائل المتبادلة بين أجهزة الاتصال العسكرية خاضعة لعملية تكويد وتشفير آلية لا يتدخل فيها العامل البشري.

د. إضافة إمكانية عقد المؤتمرات المسموعة أو المسموعة والمرئية بين القادة عبر الأثير وكلٌّ منهم موجود في مركز قيادته بين جنوده، وذلك من خلال شبكة الاتصالات الرقمية العسكرية والكاميرات التليفزيونية. وهذا النوع من الاتصالات لا يحتاج إلى إمكانات إضافية لشبكة الاتصالات العسكرية، بل يستغل إمكاناتها الذاتية.

هـ. سيطرة الحاسب الآلي على تخطيط الاتصالات وتنظيمها، وتوزيع الأحياز الترددية دون أي تدخل بشري، فالقائد العسكري أوالمستخدِم بصفة عامة ما عليه إلا أن يطلب تحقيق الاتصال

بالطرف الآخر من خلال الهاتف، أومن نهاية طرفية للحاسب الآلي أو أي وسيلة أخرى دون أن يهتم هو أو أيّ من معاونيه بكيفية ووسيلة الاتصال، إذ يقوم الحاسب الآلي بتنفيذ المهمة بعد تقويم تأثير العديد من المتغيرات التي تؤثر في عملية الاتصال، مثل طبيعة الأرض، وحالة الطقس، والوقت من الليل والنهار، وكثافة حركة تبادل الرسائل، ومدى تدخل العدو على قنوات الاتصال العاملة بالأعمال الإلكترونية المضادة وغيرها. وسيكون اختيار الحاسب الآلي للمسار ووسيلة تنفيذ الاتصال هو الاختيار الأمثل في لحظة طلب الاتصال، كما سيكون أكثر الوسائل أمنًا وسرية (السعدي،1997: 98).

و. إتاحة استخدام البنية الأساسية للاتصالات المدنية أو أجزاء منها لتحقيق الاتصالات العسكرية، دون أي تفريط في متطلبات الاتصالات العسكرية من حيث السريّة والأمن والسرعة والكفاءة.

التقنية في أنظمة التتبع:

حدث في الآونة الأخيرة تحول كبير في القوات المسلحة في معظم دول العالم، من ناحية تصميم المستشعِرات وأنظمة التتبع، ويعود هذا التحول إلى ثلاثة أسباب رئيسية (خالد، 1990: 57):

1) أصبحت الأسلحة اليوم أكثر دقة وتأثيرًا من تلك التي استخدمت في الحروب السابقة وحتى القريبة، كما أنّ الإصابات المباشرة للسفن والطائرات والمدرعات أصبحت اليوم ممكنة أكثر مما كانت سابقًا.
2) تُعَدّ تكاليف معظم الأسلحة الحديثة باهظة، بحيث إنّ إجراءات خفض النفقات في معظم دول العالم تتجه إلى الحدّ من كمية إنتاج هذه الأسلحة.
3) بما أنّ الإصابة المباشرة أصبحت شبه مؤكدة، فإنّ الخصم الذي يستطيع رؤية عدوه أولًا، ويبادر بإطلاق النار عليه تكون له الفرصة الأكبر لكسب المعركة. سرَّعت هذه العوامل في تطوير تقنية الكهروبصريات التي أدّت بدورها إلى تحسينات جوهرية في الكفاءة القتالية لجميع الأسلحة مثل المدرعات، والدفاع الجوي، والمروحيات، والمشاة، والطائرات الموجَّهة دون طيار.

تقوم الأنظمة الكهروبصرية بإنتاج الأشعة أو التقاطها باستخدام مُذبذِبات متطورة، وكاشفات حساسة جدًا. ويقع حيّز اهتمام العلماء والمهندسين المصممين لأنظمة الأسلحة الكهروبصرية ما بين الأطوال الموجية من (0.3 – 15 ميكرونًا)، وهذا الحيز هو الأكثر استخدامًا من الناحية العملية في التطبيقات العسكرية بسبب الظروف الجوية وأنواع الأهداف المحتَمَلة، إلّا أنّ هناك بعض التطبيقات العسكرية الخاصة تستخدم الأطوال الموجية للأشعة فوق البنفسجية والأشعة تحت

الحمـراء. وهنـاك نوعـان مـن التقنيـات في مجـال الأنظمـة الكهروبصـرية الحديثة هما أنظمة الرؤية الحرارية، وأنظمة الليزر، وكلٌّ منهما - عـادةً - جـزء مـن نظـام معقـد مثـل نظـام لقيـادة النيـران أو اكتشـاف الأهـداف (البصيلي، 1989: 102).

تقنية الرؤية الحرارية:

تُعَدّ أنظمة الرؤية الحرارية معدات كهروبصرية سلبية مُصمّمة لالتقاط الأشعة تحت الحمراء الصادرة من كلٍّ من الهدف والخلفية (الملحق «ب» يبين مفهوم الاشعة تحت الحمراء)، ويقع حيز الأطوال الموجبة من (3 - 5 ميكـرون، أو مـن 8 - 14 ميكرونًـا). وهـذه الأطـوال الموجيـة هـي التي يحدث لها أقل تَـوهين أثناء انتشارها في الغلاف الجوي الأرضـي. تُجَمّـع الأشـعة بواسـطة تلسـكوب خـاص ذي عدسـات مصنوعة إمّـا مـن عنصر الجرمانيوم أومن عنصر السليكون، حيـث تركـز العدسـات الأشـعة على كاشف حساس، وتمر إشارة الكاشف بعـد ذلـك في دوائـر إلكترونيـة معقدة حتى تظهر صورة حية على شاشـة تليفزيونيـة. وعلـى ذلـك يعمـل جهاز الرؤية الحرارية محولًا الأطوال الموجبة من الأشعة تحت الحمراء إلـى حيّز للموجـات المرئيـة. وتتيـح تقنيـة الرؤيـة الحراريـة الرؤيـة أثنـاء الظلام التام، وخلال الضباب والدخان، ولا تتـأثر بتـداخل أشـعة الشـمس أو المشاعل أوالأضواء الكاشفة. ويتكون جهاز الرؤية الحرارية عـادة مـن

الكاشف، ونظام المسح الخاص، بالإضافة إلى التلسكوب، والدائرة الإلكترونية، وشاشة الرؤية، وجهاز تبريد الكاشف (خالد، 1990: 97).

لقد كان المسرح العسكري أكبر مجال لتطور تقنية الرؤية الحرارية. وتنحصر المتطلبات الحالية والمستقبلية لهذه الأنظمة في مدى أطول للكشف والتمييز في الأحوال الجوية السيئة، والعمل على أن تكون هذه الأنظمة أقل وزنًا وتكلفة واستهلاكًا للطاقة وذات كفاءة أعلى. وأدى هذا إلى إنتاج كاشف أكثر حساسية، ومصفوفات ذات أعداد أكبر من العناصر الحساسة، وإلى تصميمات أدق تستخدم مواد أخف ودوائر كهربية أقل استهلاكًا للطاقة، ومبردات أكثر كفاءة. وقد أحدَث استخدام معدات الحرب الإلكترونية في الحروب الحديثة تطورًا هائلًا في مجالات هذه الحروب ومراحلها، وأصبَح الحَسْم في المعارك الحديثة لصالح الجيوش والقوات التي تستخدم الأحدث منها، وبقدر ما يَمتلكه كلُّ طرفٍ من الأطراف المتصارعة، بعد أن كانت تُحسم لمصلحة الطرف الذي يمتلك التفوق العددي، أو النوعي، أو يمتلك الأسلحة البعيدة المدى. والدليل على ذلك أنّ معدات الحرب الإلكترونية المستخدمة في الطائرات المقاتلة يقترب ثمنُها من نصف أو أقلّ من قيمة الطائرة.

تقنية الليزر:

يتم استخدام نُظم تقدير المسافة بالليزر وبواعث الأشعة في مسرح العمليات في الحروب البرية أو الجوية لتحديد الأهداف، وتوجيه وإدارة نيران الأسلحة بدقة عالية، فضلًا عن استخدام نُظم الذخيرة الموجَّهة بالليزر أو التليفزيون أو الأشعة، كما تتطلَّب معركة الأسلحة الحديثة كذلك استخدام مستشعِرات تضمُّ شبكة حاسبات إلكترونية ترصد المعلومات للأهداف، وتُحلِّلها ثم توجِّه نيران الأسلحة المختلفة نحوها لتدميرها، وهذه المستشعِرات ذات تأثير مغناطيسي أو حراري أو صوتي أو ضوئي، للكشف عن تحركات الأسلحة والمعدات في ميدان القتال البري والجوي.

ظهر أول جهاز ليزر عام 1958، وكلمة ليزر (LASER) اختصار لعدة كلمات تعني «تكبير الضوء بواسطة الانبعاث الحَثّي للأشعة»، وهذا يعني أن أشعة الليزر لها الخواص نفسها من حيث التركيز في اتجاه دقيق، والقطبية، وزاوية الطور، والطيف مثل الطاقة الباعثة لها، مما يعطي شعاع الليزر الخاصية المتفردة من حيث أحادية اللون، والتردد، والإشعاع في خط مستقيم، بشعاع مُركَّز له قدرة عالية.

أصبحت معظم القوات المسلحة في العالم في الوقت الراهن في حاجة إلى نظام إنذار وتتبع جوي مدمج ومتحرك ومتكامل، ومثل هذا النظام عليه اعتراض الهجوم المنخفض الذي تنفذه طائرات المعاونة الجوية

القريبة والمروحيات والصواريخ، ولتحقيق ذلك يستخدم ليزر نبضي سريع لقياس المسافات مع كاميرات تليفزيونية ومستشعرات للرؤية الحرارية وأجهزة تتبع كهروبصرية وأجهزة حاسبات سريعة، وهو ما يُكَوّن نظام قيادة النيران لكلٍّ من صواريخ ومدافع الدفاع الجوي. وتستخدم أغلب الأنظمة حاليًا ليزر عند الطول الموجي (1.54 ميكرون)، وتستخدم نظم الدفاع الجوي رادار ليزر ثاني أكسيد الكربون، بالإضافة إلى أجهزة الرادارات التقليدية المعروفة. ويتميز رادار الليزر بأنّ له طولًا موجيًا أقلّ، وهو ما يعطيه قدرة تحليلية أكبر في المسافة أو الزمن، كما أنّ له حساسية أكبر في قياس سرعة الأهداف، ويمكنه إعطاء صورة للهدف الملتقَط (خليل، 2001: 83).

تستخدم كلٌّ من أجهزة الرؤية الحرارية والليزر جزءًا من أسلحة المشاة ومعدات منفصلة لصالحها، وقد دخلت هذه المُعِدّات الخدمة فعلًا في معظم الجيوش الحديثة، ومن أمثلة ذلك جهاز ليزر تقدير المسافة الصغير المحمول باليد الذي يصل مداه إلى (20 كم). وتحتوي الأجيال القادمة من أنظمة الليزر للمشاة على أجهزة إضافية واقية للعين، وهي صغيرة ورخيصة الثمن ومثالية للاستخدام اليدوي، كما ستتسم هذه الأجيال بالأداء الأفضل والحجم الأصغر. ومن المنتظر ظهور معدات رؤية حرارية تعمل في الحيز من (3–5 ميكرون) لمساعدة المشاة المترجلة في العمل ليلًا بكفاءة. وسوف تكون أنظمة الليزر والفلير

الخاصة بالمشاة – على وجه العموم – قليلة التكلفة وخفيفة الوزن وذات كفاءة عالية (البصيلي، 1989: 113).

ربط الإنترنت بالشبكات الداخلية للقوات المسلحة:

توجد في وزارات الدفاع والقوات المسلحة الكثير من الأنظمة والشبكات الداخلية، وكلّ شبكة لها خواصها وميزاتها من حيث مجالات الاستخدام والمعلومات والبيانات المتوفرة في هذه الشبكات، وكذلك الوحدات المستخدمة لهذه الأنظمة. ومن الأمثلة على هذه الشبكات نظام القيادة والسيطرة والاتصالات والحاسب الآلي (C4I)، ونظام الإمداد والتزويد اللوجستي، ونظام إدارة القوى البشرية، ونظام المالية وإدارة الرواتب، ونظام إدارة المستشفيات العسكرية، وأنظمة تبادل المعلومات الاستخبارية بين مختلف أفرع القوات المسلحة. وترتبط هذه الأنظمة في كثير من دول العالم بشبكة اتّصالات، وتعمل في بعض الدول مستقلة، لكنّها تستخدم نفس شبكة الاتصالات (شلبي، 2002: 14). وعليه يمكن تقسيم شبكات المعلومات – اعتمادًا على المنطقة الجغرافية التي تغطيها الشبكة – إلى نوعين هما :

أ. **الشبكات المحلية (LAN):** وهي مجموعة من الحواسيب الشخصية المرتبط بعضها ببعض بواسطة خطوط الاتصال، حيث تتشارك هذه الحواسيب في المعدات والبرمجيات والمعلومات. وتكون حواسيب هذا

النوع من الشبكات في مكتب أو بناية واحدة أو في مجموعة بنايات متقاربة حيث يمكن لأيّ حاسوب الاتصال مع حاسوب آخر في الشبكة باستخدام مختلف مصادر ذلك الحاسوب. وبهذا نجد أنّ أهمية الشبكة المحلية تتمثل في مجموعة الحواسيب المرتبطة بها، وتستطيع استخدام جميع مصادر الشبكة، كأن تشترك جميع حواسيب الشبكة في استخدام طابعة واحدة أو المشاركة بين الحواسيب باستخدام وحدات التخزين المساندة (الأقراص)، مما يوفر الوقت والمال والجهد.

ب. **الشبكات واسعة المجال (WAN)**: تتكون من الحواسيب ووحدات طرفية متباعدة جغرافيًا ومربوطة بواسطة خطوط الاتصال. ويمكن لهذا النوع من الشبكات أن يربط بين حواسيب موجودة في مدن أو أقطار متباعدة ومختلفة. وترتبط هذه الحواسيب بحواسيب مركزية خادمة (SERVER) وتكون - بالتالي - عبارة عن شبكة من مجموعة شبكات. وفي القوات المسلحة يربط هذا النوع من الشبكات بين الوحدات والمعسكرات، وبينها وبين القيادة العامة. ويفضل وجود مزود في كلّ وحدة لتفادي تعطل المزود الرئيسي.

يمكن ربط الشبكات الموجودة في القوات المسلحة بشبكة المعلومات العالمية لتقليل عدد أجهزة الحاسب الآلي في المكاتب التي تتطلب وجود الإنترنت ووجود الأنظمة الأخرى في مكاتبها. ولكي تتم عملية الربط لا بدّ من أن تكون هذه الأنظمة قادرة على التخاطب وتبادل

المعلومات فيما بينها، ويجب توفر مجموعة من الأجهزة والبرامج للربط والاتصال مع الشبكة وفق الآتي (شوقي، 2003: 17):

- يجب توحيد أنظمة التشغيل والبروتوكولات المستخدمة في جميع الأجهزة.
- توفر أجهزة الاتصالات الطرفية القادرة على نقل المعلومات بين هذه الأنظمة.
- يكون محلل الشيفرة وسيطًا بين جهاز الحاسوب وخطّ الاتصال، بحيث يقوم بتحويل المعلومات الرقمية الخارجية من الحاسوب إلى موجات يمكن إرسالها عبر خط الاتصال، وتحويل الموجات الداخلة إلى جهاز الحاسوب من خط الاتصال إلى معلومات رقمية.
- تحتاج برامج وأجهزة الحماية إلى أجهزة وبرامج خاصة لحماية الأنظمة من الاختراقات الخارجية لتستطيع استخدام شبكة المعلومات.

تتميز أنظمة المعلومات المستخدمة في القوات المسلحة بسرية المعلومات المتوفرة فيها، على عكس المعلومات المتوفرة في الإنترنت، إذ تبقى شبكة الإنترنت غير آمنة، وتتعرض للاختراقات وكثرة الراغبين في الحصول على المعلومات من الأجهزة التي ترتبط بها، لذلك لا بدّ من وجود قوانين وتشريعات وسياسات لحماية هذه الأنظمة من التهديدات

الخارجية إذا تطلّب الأمر الربط بالشبكة، نظرًا لما تحتويه شبكات القوات المسلحة من معلومات هامة جدًا يحاول الأعداء الحصول عليها. كما ينصح خبراء أنظمة المعلومات بتوخي الحذر الشّديد، لأن الحديث عن الأمن في الإنترنت لا يمكن الوثوق بأنّه آمن من الناحية الفنية، ولذلك يبقى الحذر البشري مقدَّمًا في هذا الجانب.

البعد الأمني لاستخدام الإنترنت في القوات المسلحة:

تستعمل الجهات العسكرية شبكة الإنترنت على نطاق واسع كوسيلة للاتصالات الخارجية أو الداخلية، حيث يُحَسّن ذلك مستوى أداء هذه الجهات من خلال المشاركة في المعلومات، وتوفير الإنفاق على تطوير أنظمة الاتصالات التقليدية. وبذلك يتعامل العسكريون مع جهات التوريد الخارجية عبر الإنترنت بالإضافة إلى المجالات السابق ذكرها.

تُعتبر شبكة الإنترنت وسيلة مهمة جدًا من إفرازات التكنولوجيا الحديثة في مجال الاتصالات والتراسل، لكنّها لا تخلو من أوجه التهديد على القطاعات العسكرية، لذلك ظهرت سلبيات كثيرة جدًا إلى جانب الفوائد المرجوة منها، كما أنّ لها أخطارًا وتأثيرًا كبيرًا على الأعمال اليومية في القوات المسلحة، لذلك يجب تحديد استخدامها ومعرفة الغرض من وجودها في المكاتب، وضبط المعلومات التي يمكن أن تُرسَل عن طريقها، والمعلومات التي يمكن السماح بوجودها وتصفحها، وذلك

للمحافظة على طبيعة السرّية في القوات المسلحة. ومن المخاطر المترتبة على ذلك ما يلي:

1. يتميز عمل العسكريين بالسرّية، ولذلك فإن المعلومات التي يتم تبادلها، والتي قد تبدو للبعض - بحكم استخدامهم اليومي لها وتعودهم عليها - بأنها معلومات عادية، قد تكون في الواقع معلومات خطيرة وهامة يمكن أن يستفيد منها الأعداء في حال وقوعها بين أيديهم.
2. يمكن اختراق أنظمة المعلومات بسبب جهل البعض بأصول أمن المعلومات ونوعية المعلومات التي يمكن إرسالها أو حفظها على الجهاز المربوط مع الإنترنت.
3. نفاذ بعض الأشخاص المشتركين في الشبكة إلى بعض الشبكات المحلية للمؤسسات والدوائر العسكرية، حيث يمكنهم قراءة وتصفح البريد الإلكتروني لهذه المؤسسات واستخدامه لأغراض شخصية قد تضرّ بها، والاطلاع على البيانات المُخزَّنة على أجهزة الحاسوب الخاصة بها، وتعطيل برامج التشغيل أو التخزين، وتغيير المعلومات المُخزَّنة عليها، وسرقة كلمات المرور السرية للدخول إلى الأنظمة.

• نماذج تطبيقية لاستخدام الأدوات العسكرية للحرب الإلكترونية

الحرب العالمية الأولى:

يمكن اعتبار الحرب العالمية الأولى وما تخللها من حوادث إلكترونية هامة البداية الحقيقية للحرب الإلكترونية. فقد ازدادت تقنية الحرب الإلكترونية في بداية الحرب العالمية الأولى، إذ قامت السفن الألمانية بالتشويش على العديد من الأمواج اللاسلكية التي كانت البحرية البريطانية تتداولها، واستطاع الألمان التأثير على سير العمليات البحرية البريطانية العاملة قرب السواحل التركية، وعلى عمليات قصف الأسطول البريطاني لميناء سيفاستبول. وفي مقابل ذلك قامت أجهزة لا سلكية بريطانية بتحديد مصدر أجهزة الإرسال اللاسلكية الألمانية بواسطة المحطات اللاسلكية، تدعمها أجهزة مُحدِّدات الاتجاه التي ساعدت على استمكان موقع الأسطول الألماني ووجهت سفنها إلى أنسب نقطة للالتقاء معه (خالد، 1990: 33).

ففي عام 1914، وبعد إعلان بريطانيا الحرب مباشرة على ألمانيا، وقعت حادثة مهمة في البحر المتوسط، وذلك عندما شاهد الطراد البريطاني (غلوسيستر) الطرادين الألمانيين (جونين) و(براسلو)، وكانت مهمة الطراد البريطاني الإبلاغ لاسلكيًا عن جميع تحركات السفن

الألمانية إلى قيادة البحرية في لندن لتوجّه الأوامر إلى أسطول المتوسط باعتراض الطرادين الألمانيين وتدميرهما، ولسوء الحظ لم يكن لدى الإنكليز أية فكرة عن وجهة الطرادين اللذين يمكن أن يتجها إلى إيطاليا التي كانت محايدة في ذلك الوقت أو إلى ميناء تركي صديق، وفي تلك اللحظة تم التقاط الاتصالات اللاسلكية بين الطراد (غلوسيستر) وقيادة البحرية البريطانية من قبل الطرّادين الألمانيين اللذين قررا التخلص من المطاردة، وذلك بالدخول على الاتصالات المعادية، حيث قاما بإرسال تشويش ضجيجي على التردد المستخدم من قبل الإنكليز، وحاول البريطانيون تغيير ترددهم عدة مرات دون جدوى، وفجأة غيرت السفن الألمانية وجهتها، وانطلقت بكامل سرعتها إلى المياه التركية الصديقة، وقد اعتُبِر هذا التشويش على الاتصالات الإنكليزية أول عمل حقيقي للحرب الإلكترونية، حيث تم لأول مرة في التاريخ استخدام الأمواج الكهرطيسية ليس لأغراض الاتصال فقط، بل للتشويش على الاتصالات المعادية (الأشرم، 1988: 36).

ولذلك أصبح المهندسون والفنيون العسكريون في الحرب العالمية الأولى يكرسون جهودهم لبناء معدات أكثر تطورًا، ليس لتحسين الاتصال بين وحداتهم فقط، بل لاكتشاف محطات العدو اللاسلكية وتحديد مواقعها، وتمّ لهذا الغرض تصميم جهاز تحديد الاتجاه الذي أصبح أداة ثمينة في التجسس الإلكتروني والحصول على المعلومات حول العدو.

وكان العثور على موقع محطة بثّ معادية يدل دائمًا على وجود وحدة عسكرية كبيرة، علاوة على أن التوزيع الأرضي لمحطات اللاسلكي كان يعطي صورة واضحة عن تنظيم جبهة العدو، بينما كانت التغيرات في مواقع محطات اللاسلكي تعطي إشارة دقيقة نوعًا ما حول تحركات العدو. وقد تميز البريطانيون والفرنسيون بشكل خاص بجودة التنظيم في هذا المجال، إذ استخدموا منذ عام 1915 أنظمة الاعتراض الفعالة القائمة على تحديد زوايا البث اللاسلكي التي مكنتهم من تحديد مواقع وحدات العدو الكبرى، ومراقبة تحركات القوات حسب خطط الهجوم، وقد ساهم ذلك كثيرًا في نجاح الحلفاء في إرهاق العدو وإجباره على اتخاذ وضع ساكن عانى فيه نسبة إنهاك عالية.

ومن جهة أخرى تمكنت المخابرات البريطانية من التنصت على الرسائل الدبلوماسية وحلّ شيفرات الكود للجانب الألماني، وتمكن البريطانيون لمدة ثلاث سنوات متتالية أثناء الحرب العالمية الأولى من حلّ الشيفرة في الرسائل المتبادلة بين وزير الخارجية الألمانية وسفراء ألمانيا في أوروبا، وقد حاول البريطانيون إبقاء هذا سرًا لا يعرفه أحد من حلفائهم في أمريكا، فيما عدا المعلومات التي تلقوها عن محاولة ألمانيا الزج بالمكسيك في الحرب، مع إعطاء وعود لها بأحقيتها في احتلال تكساس وأريزونا ونيومكسيكو.

الحرب العالمية الثانية:

يُعَدّ استخدام الإلكترونيات إحدى أبرز السمات الجديرة بالملاحظة في الحرب العالمية الثانية، وقد أطلق عليها ونستون تشرتشل الاسم الرنان (الحرب السحرية)، فقد ركز خبراء الجاسوسية الإلكترونية جهودهم أثناء الحرب العالمية الثانية على الاتصالات اللاسلكية المعادية، ووسائل الملاحة الإلكترونية والرادار، وليس مستغربًا أنّ دور اعتراض إشارات العدو اللاسلكية، واستخدام مُحددِّات الاتجاه اللاسلكي في الحرب العالمية الثانية كان أكبر من دوره في الحرب العالمية الأولى (برم، 2010: 72).

لقد ابتكر الألمان في هذه الحرب أسلوبًا جديدًا في القصف الجوي الليلي، فقاموا بإرسال حزم لاسلكية موجهة نحو العاصمة لندن من موقعين أرضيين يقعان في ساحل الأراضي المحتلة في فرنسا وبلجيكا، ويتقاطعان عند الهدف (لندن)، وأخذت الطائرات القاصفة الألمانية تتعقب إحدى الحزمتين، وعند وصولها إلى نقطة التقاطع مع الحزمة الثانية تمثل بإرسال حزمة لاسلكية ضيقة تلتقي مع إحدى الحزمتين اللاسلكيتين اللتين ترسلهما الأجهزة الألمانية، وجعلها تتقاطع في منطقة تقع خارج لندن، الأمر الذي دفع القاصفات الألمانية إلى إسقاط قنابلها عند تلك النقطة بعيدًا عن الهدف. وعندما قام الألمان في هذه الحرب

باستخدام التنصت على الشبكات اللاسلكية البريطانية، أخذ البريطانيون يشوشون عليها بموجات لاسلكية مماثلة (خالد، 1990: 34).

ولعل حادثة غرق السفينة الألمانية (بسمارك) التي كانت مكلَّفة بالإغارة على السفن التجارية البريطانية عام 1941 من أهم النماذج التطبيقية على الحرب الإلكترونية في الحرب العالمية الثانية، حيث استطاعت سفينة بسمارك الألمانية - بفضل أجهزة الرادار التي تمتلكها - التغلب على السفن الحربية البريطانية التي أخذت موقع الهجوم على سفينة بسمارك في المضيق الدانماركي في المحيط الأطلنطي، ولكنّ الاتصال اللاسلكي الذي استمر لمدة نصف ساعة ما بين قائد سفينة بسمارك وقياداته الألمانية أدى إلى كشف موقع السفينة وتحديد اتجاهها من قبل طائرات الاستطلاع البريطانية، وبعد ذلك تم إرسال السفن الحربية البريطانية إلى الموقع بعد إصابة جهاز الرادار في سفينة بسمارك، وتمكنت من محاصرتها وإغراقها ومعظم طاقمها، وقد كان ذلك كلّه نتيجة خروج السفينة بسمارك عن قاعدة الصمت اللاسلكي، وهي أهم قواعد الحرب الإلكترونية آنذاك. واعتُبِرت هذه العمليات أول نموذج تاريخي للسباق في مجال الحرب الإلكترونية.

ومن أبرز حالات هذا السباق الردّ البريطاني على الرادار الألماني (فورست بورج) الذي كان يسدد المدافع بالتنسيق مع رادارَي (فريبا) و(لشتن شتاين)، حيث ألّفَت تلك الرادارات كلّها جهازًا دفاعيًا مضادًا

لقاذفات القنابل. ولإبطال مفعول الرادارات الألمانية قام البريطانيون باستخدام رقائق معدنية تُلقى في الجوّ لتقوم بعكس الأمواج الرادارية، مما ساعد على تضليل الألمان وحجب استمكان الطائرات البريطانية الحقيقية.

ولقد أثبت العديد من المعارك في الحرب العالمية الثانية أهمية الدروس المستفادة من الاستعانة بوسائل الحرب الإلكترونية، ولم يكن يكفي التنبؤ بما لدى العدو، بل كان مطلوبًا أيضًا التكهن بنواياه مستقبلًا، فقد اتخذ الألمان آنذاك قرارًا حكيمًا عندما قرروا الطيران على طول السواحل البريطانية، فكانوا أول من قام بنوع من الاستطلاع الإلكتروني في التاريخ لاستطلاع ما لدى بريطانيا من وسائل الحرب الإلكترونية الحديثة، كما خصصت ألمانيا بعض طائراتها لاستطلاع الإشعاعات الإلكترونية في سماء بريطانيا، وكان لديها القدرة على إنتاج إلكترونيات واستخدامها في التقاط الاشعاعات الصادرة عن المعدات البريطانية الرادارية أثناء إجراء اختبارات عليها.

حرب الخليج (1990-1991):

كانت حرب الخليج - التي شهدت استخدامًا غير مسبوق للأقمار الصناعية لأغراض الاتصالات والملاحة والاستخبارات - من أهم تطبيقات الحرب الإلكترونية. فقد زودت الأقمار الصناعية الأمريكية الثابتة بالنسبة إلى الأرض والمخصصة للاستخبارات الإلكترونية القادة

الميدانيين بالمعلومات الفورية، لأنّ الاتصال المتطور بين مقارّ معالجة البيانات المتمركزة في أمريكا والمقارّ الموجودة على مسرح العمليات، تَوفَّر بحلول منتصف ثمانينيات القرن العشرين، بفضل برامج الاستكشاف الثابت والتكتيكي للقدرات الوطنية التي سرّعت تدفق الاستخبارات إلى حدّ كبير. وشملت مواقع الاستخبارات الإلكترونية الاستراتيجية المتمركزة على الأرض – التي استخدمت في الاستخبارات الموجَّهة ضد العراق – محطات أمريكية في تركيا والمملكة العربية السعودية ودولة الإمارات العربية المتحدة وسلطنة عمان، بالإضافة إلى محطات بريطانية في قبرص، ومقارّ فرنسية في جيبوتي (staff، 1991: 330).

وقد تعززت قدرات قوات التحالف البرية في تدابير المساندة الإلكترونية إلى حدّ كبير بفعل قدرات الجيش الأمريكي في الحرب الإلكترونية، حيث عملت تلك القوات جنبًا إلى جنب مع ألوية الاستخبارات العسكرية على مستوى الفيالق، وظلّ هذا التكامل مستمرًا طوال الحرب بين تدابير المساندة الإلكترونية وأسلحة الحرب الإلكترونية والقتل العنيف ذات الطابع الهجومي، وتجميع الخلية للمعلومات الاستخباراتية. وفي المقابل اقتصر استخدام العراق معلومات استخبارات الاتصالات على نقل الصواريخ وإبعادها عن مرمى الضربات الجوية، وتجنُّب الضربات الموجهة إلى الرادارات لإخماد وسائل الدفاع الجوي.

تمّت خلال العملية المعروفة بـ«درع الصحراء» برمجة أجهزة محاكاة الحرب الإلكترونية الأمريكية الرئيسية - وهي جهاز التحليل والمعالجة الآنية المضبوط رقميًا (Redcap) وجهاز محاكاة تقييم الحرب الإلكترونية الجوية (afewes)- بصورة مفصلة عن منظومة الدفاع الجوي العراقية، ثم جرى اختبار كلّ تكتيك وكلّ جزء مرتبط من معدات الحرب الإلكترونية على أجهزة المحاكاة لقياس مدى فعاليتها. وكانت معظم أجهزة الرادار المستخدمة في المنظومة العراقية من الأنواع السوفيتية، وتخضع فعالية الحرب الإلكترونية ضدها للبحث والتحقيق منذ سنوات كثيرة، وبالإضافة إلى ذلك هناك أجهزة رادار مشتراة من دول غربية، ولذلك فإنّ ضعف تلك الأجهزة وتأثيرها على النظام ككلّ ظل أقلّ تأكيدًا إلى أن بدأت أجهزة المحاكاة (redcap) و(afewes) بتقديم الأجوبة (الخليفة، 2000: 92).

وفي عملية عاصفة الصحراء في 17 يناير 1991، بدأت الولايات المتحدة الأمريكية التشويش على ترددات الاتصالات اللاسلكية في العراق تمهيدًا للهجوم الجوي، حيث كانت مراكز ومنشآت القيادة والسيطرة والاستخبارات في العراق الهدف الأول المحدَّد عند انطلاق الحملة الجوية، وتَمّ توجيه ضربات جوية ثقيلة ومتكررة إلى مقارّ وزارة الدفاع، ومقارّ القوات الجوية والدفاع الجوي العراقي، والمجمع الرئاسي، ومقارّ حزب البعث، والمقاسم الهاتفية، وغيرها من مرافق ومعاقل الاتصالات في بغداد وما حولها، إضافة إلى مراكز قيادة الدفاع

الجوي الإقليمية العراقية في كركوك والناصرية والرطبة، وغيرها من مراكز السيطرة والاستخبارات الرئيسية، مثل بيجي وكركوك والكوت، والجسور القائمة على نهر دجلة التي تحمل كابلات الاتصالات، ومحطات الاستخبارات الإشارية والتشويش العراقية، ومنشآت بريد واتصالات القيادة الأخرى عبر الدولة. وحسب الجنرال شوارزكوف، قائد قوات التحالف في الخليج، هوجمت 75٪ من مراكز القيادة والسيطرة والاتصالات في العراق خلال أربعة عشر يومًا من الحملة الجوية، وتم تدمير وإضعاف ثلث تلك الأهداف تقريبًا. وبالإضافة إلى الضربات الجوية، نفذت نخبة الكوماندوز الأمريكية والقوات الخاصة البريطانية والفرنسية عمليات داخل بغداد لتدمير شبكة أسلاك الاتصالات تحت الأرضية الواصلة بين بغداد والقوات العراقية الموجودة على مسرح العمليات الكويتي (Eric، 1991: 9).

أمّا فيما يخص التجسس الإلكتروني في تلك الحرب فقد كان للولايات المتحدة الأمريكية وحلفائها مصادر تجسسهم الخاصة التي اشتملت على صور من الأقمار الصناعية، وطائرات تجسس دون طيارين. وفي عام 1990 استطاعت الأقمار الصناعية الأمريكية للتجسس اكتشاف قوات عسكرية عراقية كبيرة على الحدود الكويتية، فقبل أن تندلع الحرب، استطاعت نظم المسح للأقمار الصناعية رسم صور وخرائط لمناطق الأهداف المحتملة، وقد وُضِعت هذه الخرائط على متن نافذة الصواريخ توماهوك أثناء الحرب، وقورنت بالصور التي التُقِطَت بواسطة رادار قاذفة الصواريخ ذاتها. وقد

ساعد نظام تحديد المواقع الكوني GPS– وهو نظام يتألف من مجموعة 24 قمرًا صناعيًا تصدر إشارات تستخدم لتحديد المواقع – ساعد القوات الأرضية للحلفاء على التحرك الصحيح في التضاريس الصحراوية (البداينة،2002:194).

وقد استُخدِم نظام تحديد المواقع الكوني من قبل الطائرات لمسح الحقول الأساسية بمنتهى الدقة، ومن قبل السفن الحربية الأمريكية للحصول على الإحداثيات الصحيحة لإطلاق الصواريخ، وقد حلقت الطائرات دون طيار ودارت فوق أرض المعركة مستخدمة جهاز تصوير فيديو وجهاز مسح إلكتروني يعمل بالأشعة فوق الحمراء، لتوفير بيانات تكتيكية قتالية حقيقية تبين تحركات الجنود العراقيين وتقديرات القصف، وقد قامت هذه الطائرات بطلعات بلغت 530 مهمة، وبمعدل 1700 ساعة طيران فعلية (Mazar, Snider, Blackwell، 1993: 68).

ويمكن اختصار أهداف السياسة الإلكترونية لقوات التحالف المستخدَمة في حرب الخليج على جميع مستويات العمليات كما يلي:

1. تحييد قدرة العدو على توجيه العمليات بأكبر درجة ممكنة، وإضعاف التماسك القتالي على مستوى التشكيلات والوحدات لمنع احتمال وجود مقاومة مترابطة.
2. تعطيل جميع أجهزة المراقبة العراقية بالكامل، بحيث يتم حرمان هرم القيادة العسكرية من المعلومات الاستخبارية حول أرض المعركة، التي

تعتمد خططهم عليها، وفي الوقت ذاته تأمين حرية الحركة لمصادر قوات التحالف.

3. إضعاف قدرة العدو على القتال من خلال تحييد جميع عمليات البث الإلكتروني الفعالة المصممة للمساعدة في تحديد الأهداف.
4. الحصول على المعلومات الاستخبارية الإلكترونية قبل المعارك وأثناءها وبعدها، لتوفير المعلومات اللازمة لوضع الخطط وشنّ الحرب لجميع المعارك المستقبلية.
5. تعزيز قدرة القتال الخاصة لدى جميع منظومات السلاح الصديقة.
6. توفير اتصالات آنيّة آمنة، ومقارنة البيانات للسماح بإدارة سلسة للعمليات.
7. تعزيز المصادر لضمان زخم القوة الميدانية والعمليات على مدار الساعة.
8. عزل مسرح الحرب عن التدخل الإلكتروني الخارجي.

الحروب الإسرائيلية- العربية:

قامت مصر وسورية والعراق والأردن في عام 1967 بنشر ما يقارب 250,000 جندي، و 700 طائرة مقاتلة، وأكثر من 2000 دبابة على طول الحدود مع إسرائيل، جاهزة للهجوم من جميع الجهات، مما حدا بالعالم أجمع توقع حدوث حرب عالمية ثالثة. وقد ركزت أنظمة جمع المعلومات المختلفة للقوى العالمية الرئيسية على الوضع في الشرق الأوسط، ففي البحر الأبيض المتوسط كانت سفن الأسطول السوفييتي - ولا سيّما تلك المعدَّلة خصيصًا للتجسس الإلكتروني - مستعدة باستمرار لتلقي جميع ترددات

الطيف الكهرطيسي لمراقبة الوضع، وكان الأسطول السادس الأمريكي يطوف المياه الشرقية في البحر المتوسط، إضافة إلى طائرات خاصة مجهزة بأكثر الأجهزة الإلكترونية تطورًا، ووُضِعَت إسرائيل وسيناء، - وفي الواقع - منطقة الشرق الأوسط بأكملها تحت المراقبة الدائمة، وقامت سفينة الاستخبارات في البحرية الأمريكية USS Liberty بدوريات مستمرة في مهمة لجمع المعلومات الاستخباراتية مقابل سواحل فلسطين المحتلة، وهي مجهزة بمعدات إلكترونية حساسة للغاية، يمكنها اعتراض وتحليل شيفرة جميع الاتصالات اللاسلكية التي كان يبثها العرب والإسرائيليون، وقامت بتحليل جميع رسائل راداراتهم (برم، 2010: 216).

وفي الجانب المصري كانت جميع محطات الرادار المصرية في وضعية الاستعداد، وكان عددها جميعًا 23 محطة، منها 16 محطة في شبه جزيرة سيناء. وكان الفضاء الجوي والسواحل المحيطة بمصر مغطاة بشبكات رادار الإنذار المبكر فيها، وكانت شبكات الرادار الإسرائيلية في حالة استعداد دائم كذلك (خليل، 2002: 48).

وقد شهد يوم 5 حزيران 1967 بداية حرب الأيام الستة التي كانت بمثابة سلسلة من التحديات الإلكترونية التي استمرت سنوات عديدة، فقد نجح الإسرائيليون - من خلال التفسير الماهر للصور الاستطلاعية التي كانت تلتقطها طائرات الاستطلاع التي كانت تطير على ارتفاع منخفض، ومحطات الرادار وتغطيات الرادار حتى للبقع العمياء أو غير الواضحة - في رسم خططهم التفصيلية والدقيقة للحرب، حتى إنهم تمكنوا نتيجة ذلك من رسم

ممرات لطائراتهم بين الأبراج والمآذن في القاهرة لشنّ هجوم مباغت على المقرات والقواعد الجوية في القاهرة.

تمكن الإسرائيليون - من خلال تعطيل الرادارات والاتصالات اللاسلكية المصرية - من إرسال كلّ طائرة للقيام بالعمليات عدة مرات، وضاعفوا بذلك من عدد المهمات التي يمكن إنجازها. وبعد أن دمر الإسرائيليون 300 طائرة من القوة الجوية المصرية البالغ عددها 320 طائرة، تقدموا على الفور لتدمير القوات الجوية للدول العربية الأخرى المجاورة لإسرائيل، فتمّ تدمير القوات الجوية السورية والأردنية والعراقية في توالٍ سريع (متولي، 2001: 83).

إلّا أن المصريين كانوا أكثر تصميمًا على ألّا تتم مباغتتهم مرة أخرى في حرب عام 1973، فقاموا باستخدام ممتاز للاستخبارات العسكرية قبل اندلاع الحرب، وعملوا بمساعدة الاتحاد السوفييتي (سابقًا) على تحديث أجهزة الاستخبارات لديهم، بالحصول على مُعدّات حديثة للتجسس الإلكتروني، بما في ذلك أجهزة استقبال لاسلكي فائقة الحساسية، وأجهزة استقبال استطلاعية للرادار، وسجلات ومحددات اتجاه.

ومن أسلحة الحرب الإلكترونية التي استخدمها المصريون في حرب عام 1973 صاروخ Strela الصغير المضاد للطائرات الذي يستطيع الجندي حمله على كتفه، وكان له نوع جديد تمامًا من أنظمة التوجيه، حيث كان يستخدم الاشعة تحت الحمراء، وكلّ ما كان على الجندي أن يفعله هو تصويب الصاروخ نحو طائرة معادية تطير على ارتفاع منخفض، ومن ثم

يكشف الكاشف بالأشعة تحت الحمراء المركب في الصاروخ الحرارة المنبعثة من المحركات النفاثة في الطائرة، وينقل رسائل موضحة للمدى وزاوية الاتجاه إلى نظام التحكم والتوجيه الذي يرشد الصاروخ إلى هدفه، وهذا النظام الموجه للصاروخ يسمى mario IR homing، (1985: 191).

وقد تم استخدام تقنية جديدة هي الرادار من طراز Gun Dish المُستخدَم في المدفعية المصرية تفاديًا للإجراءات الإلكترونية المضادة، حيث كان هذا الرادار يستخدم ترددًا أعلى بكثير من أيّ تردد استخدمه المصريون في السابق، حيث لم تستطع المستقبِلات الإسرائيلية التي كانت مصنوعة لاعتراض الترددات اكتشاف الإشارات الكهرطيسية ذات الترددات العالية جدًا لرادار Gun Dish (متولي، 1985: 86).

لقد شكّلت هذه التقنيات الجديدة مع تلك الأسلحة الموجودة من قبل في القوات المسلحة المصرية نظامًا دفاعيًا جويًا استثنائيًا سمح للمصريين بالتقدم، حيث وجد الطيران الإسرائيلي المُكلَّف بمساندة القوات البرية المهاجمة للأرتال المدرعة المعادية، أنّ لا سبيل لتفادي مثل هذه الشبكة من النيران، فإذا هبطت الطائرات إلى ارتفاع منخفض لتفادي صواريخ سام فسوف تدخل حتمًا ضمن مدى نيران المدفعية الحاملة لرادار Gun Dish، أوتصبح هدفًا لصواريخ Strela الصغيرة، ولذلك كانت خسائر الجو الإسرائيلية عالية جدًا، حتى إنّ القيادات الأرضية توقفت عن طلب الدعم الجوي ضد الأرتال المدرعة العادية.

وعلى الرغم من أنّ المعارك البحرية في هذه الحرب لم يكن لها تأثير على حصيلتها، إلا أنّ الدور الذي لعبته الإجراءات الإلكترونية المضادة في هذه المعارك كبير جدًا، فالتشكيلات البحرية المتصارعة لم تصبح في مدى النظر لكلٍّ من الطرفين، بل جرى كلّ شيء إلكترونيًا، وفي كلّ اشتباك كان الطرف الذي يملك إجراءات إلكترونية أكثر فاعلية هو الّذي يخرج منتصرًا، ففي المعركتين البحريتين اللتين جرتا في اللاذقية ودمياط – بلطيم، لم يتمكن أيٌّ من الصواريخ العربية الاثنين والخمسين التي أُطلِقت على الوحدات الإسرائيلية من إصابة أهدافها، ويمكن إرجاع سبب ذلك إلى التخطيط والاستخدام الناجع لمعدات الحرب الإلكترونية من قبل البحرية الإسرائيلية، وقد ساهم ذلك أيضًا في وضع حدّ لتهديد الصواريخ لأساطيل القوى الغربية .

وسعت إسرائيل منذ ذلك الحين إلى تطوير قدراتها التقنية في مجال أسلحة الحرب الإلكترونية في الوحدات التقنية الفرعية للجيش الإسرائيلي، وزيادة درجة جاهزيتها لتوفير الحلول التشغيلية والإلكترونية لمتطلبات تكنولوجيا المعلومات والاتصالات للجيش الإسرائيلي، وتخصيص طيف الترددات المستخدَمة، وغيرها من الوظائف الرقمية والمعلوماتية التي تستخدمها في المواجهات الإلكترونية مع جميع الأطراف المعادية لها. وعلى الجانب الآخر كان هناك تغير ملحوظ في بنية المقاومة العربية ضد الوجود الإسرائيلي، فلم يعد الصراع يدار بالقنابل والصواريخ بل تحولت

الحلبة الإلكترونية إلى مسرح لتنفيذ الهجمات الإلكترونية ضد إسرائيل (مساعد، 2005: 57).

ففي حرب تموز عام 2006 دارت العديد من المواجهات الإلكترونية بين إسرائيل وحزب الله، حيث تمت إصابة البارجة الإسرائيلية (Hanit) بصاروخ أدى إلى تعطيل وظائفها، بعد قيام الوحدات الإلكترونية التابعة لحزب الله بالتشويش على الأنظمة المضادة لإطلاق الصواريخ الموجودة على متن البارجة، وقد قامت المقاومة اللبنانية أيضًا بمهاجمة الطائرات الإسرائيلية بصواريخ من نوع سام 16 التي تمتاز باستعصائها على التشويش الإلكتروني وصعوبة رصدها بأدوات التتبع البصرية، مما أعطى المقاومة اللبنانية نوعًا من التميز الإلكتروني، تَمثّل بإمكانية إفلات صواريخها المطلقة صوب إسرائيل من التتبع الرقمي والتكنولوجي، علاوة على تزويد الاستخبارات العسكرية الإسرائيلية بمعلومات مُضلِّلَة عبر اختراقها لأدوات الاتصال والتواصل الإسرائيلية، والتعتيم المعلوماتي على معلوماتها وبنك أهدافها، كما قامت المقاومة اللبنانية بتجنيد خاصية جوجل إرث (Google Earth) التي يقدمها محرك البحث العالمي جوجل، لتحديد أهدافها بدقة (العليان، 2011: 5).

تشكل الحرب الإلكترونية تحديًا أمنيًا جديدًا لإسرائيل، فنجاح مثل هذه الهجمات يعني الطعن في نظريتها الأمنية، وبالتالي التشكيك بالقادة السياسيين والأمنيين الإسرائيليين الذين أعلنوا مرارًا وتكرارًا أنّ إسرائيل تمتلك قدرة دفاعية في كافة المجالات، وأنه من الصعب المساس بها. فعلى

الصعيد الإلكتروني مثلًا، أشار «عاموس يادلين» رئيس جهاز الاستخبارات العسكرية الإسرائيلية بين عامي 2006–2010، في محاضرة له في (معهد أبحاث الأمن القومي الإسرائيلي) إلى أنّ إسرائيل تواجه خطرًا أمنيًا ومعلوماتيًا يكمن في احتمالية اختراق المواقع والحواسيب الحساسة للدولة، ولكنْ في المقابل، أكد يادلين أنّ هيئة السايبر في الجيش الإسرائيلي تمتلك القدرات اللازمة لردع أي هجوم إلكتروني، إضافة إلى مقدرة الهيئة على تنفيذ هجمات إلكترونية على أهداف معادية لإسرائيل، كما صنّف الجيش الإسرائيلي الحرب الإلكترونية كساحة خامسة للقتال، تضاف إلى الساحة البرية والبحرية والجوية والفضائية، في صورة تشير إلى الأهمية الكبيرة التي توليها إسرائيل ووحداتها العسكرية الرقمية في الجيش الإسرائيلي لظروف وأدوات الحرب الإلكترونية (إيفن، 2011: 16).

أمّا في مجال الروبوتات العسكرية فقد كشفت هيئة التصنيع العسكرية الإسرائيلية عن الانتهاء من تصنيع روبوت عسكري متطور، قادر على الدخول إلى الأنفاق، والصعود إلى الأبنية، وتصوير الأماكن الدقيقة، والقتال البري في المناطق المعتمة والموحلة، وإصدار إشارات إلى مراكز التحكم، تحدد الأهداف بدقة، وترسم المسارات بوضوح، وتستطيع العمل لساعات طويلة في أقسى الظروف وأصعبها، ويمكن برمجتها مسبقًا وتحديد مهامّها والمطلوب منها القيام به، كما يمكن تشغيلها آليًا عن بعد، والتحكم بها من خلال الصوت والصورة اللذين تنقلهما، وتحديد مهامها وتغييرها وفق المعطيات الجديدة والمعلومات المنقولة. وستكون هذه المقاتلات الآلية

في خدمة وحدة الأنفاق قادرة على خوض المعارك الخطرة، والنزول إلى الأعماق السحيقة، وتجاوز العقبات الشديدة.

وقد تم تزويد هذه المقاتلات بمفجّر ذاتي في حال اكتشافها أو محاولة السيطرة عليها، لئلا تقع في أيدي المقاومة الفلسطينية، التي قد تفككها وتستفيد من تقنيتها، كما قد تتمكن من تحليل شيفرتها الخاصة، والوصول إلى المعلومات التي جمعتها والمراكز التي نقلت إليها المعلومات وبقيت على اتصال بها، أو قد تقوم باستخدامها في الاتجاه المعاكس، وخاصةً أن قوى المقاومة الفلسطينية باتت تمتلك تقنية عالية، وعندها القدرة على الاختراق وإعادة البرمجة والتوجيه (سينجر، 2010: 180).

الحرب على الإرهاب:

أصبحت الحرب على الإرهاب على رأس أولويات السياسة الخارجية للولايات المتحدة الأمريكية والدول المكشوفة للتهديدات الإرهابية. وتركزت هذه الحرب منذ ذلك الحين على استهداف مصادر القوة المادية للمنظمات الإرهابية، ووُضِعت استراتيجيات الحرب على الإرهاب من حيث التمويل والتسليح والتجنيد على رأس الأهداف التي يجب مواجهتها بغرض إحباط الأعمال الإرهابية بشكل عام، وإرباك مراكز قيادة التنظيمات الإرهابية، ولذلك استطاعت الولايات المتحدة ودول أوروبا الغربية وغيرها، خلال الفترة الممتدة من عام 2001 وحتى الآن، تحقيق نجاح ملموس فيما يتعلق بتقزيم قوة تنظيم القاعدة والحدّ من قدرته على شنّ عمليات في الغرب .

ولكن جاء الردّ من التنظيمات الإرهابية على استراتيجية تدمير قوتها المادية بطلب تجنيد المزيد من المقاتلين لتعويض القتلى، واستجرار المزيد من الأموال لتعويض الخسائر المادية. وكذلك أدى ظهور النسخة الجديدة من التنظيمات الإرهابية في صورة تنظيم الدولة الإسلامية في العراق والشام المعروف باسم (داعش)، ثم انتشار موجة جديدة من الأعمال الإرهابية في الولايات المتحدة ودول أوروبا وغيرها من أنحاء العالم، منذ عام 2014، أدّى ذلك كلّه إلى رفع الجاهزية واستخدام التقنيات الأكثر حداثة وسرعةً في مواجهة مقومات القوة المادية للتنظيمات الإرهابية. فمع الحيل التي يعتمد عليها الإرهابيون للمواجهة على الأرض، ولجوئهم في بعض الأحيان إلى استخدام دروع بشرية من المدنيين لحماية أنفسهم، أصبح تطوير الصناعات العسكرية الوسيلة المُثلى لصيدهم وتوجيه إصابات مباشرة لهم. وتتمثل الاستراتيجية الخاصة بمواجهة القوة المادية للتنظيمات الإرهابية بأربع نقاط هي (سليمان، 2014: 13):

1. التوسع في استخدام الطائرات دون طيار في عمليات الرصد والقصف والمطاردة.
2. تكوين غرفة عمليات لمراقبة الحدود تسمح بتحرك القوات بسرعة لمواجهة أي تحركات إرهابية.
3. مراقبة الحدود البرية القريبة من معاقل التنظيمات الإرهابية باستخدام طلعات طيران دورية.
4. حرمان الجماعات الإرهابية من الحصول على الملاذات الآمنة.

ومن أهم أسلحة الحرب الإلكترونية المستخدمة لمواجهة التنظيمات الإرهابية الطائرات غير المأهولة أو ما يسمّى بالطائرات دون طيار، مثل طائرات «بريديتور» التي لا تزال تعمل فوق أفغانستان والعراق، والتي قصفت جميع أنواع الأهداف من بيوت مشتبه في استخدامها كمخابئ للمتمردين، إلى السيارات التي يتم إعدادها للهجمات الانتحارية. فقد أصبحت الطائرة غير المأهولة الآلة الأمريكية الأنشط في الجو، ونفّذت طائرة بريديتور من حزيران 2005 إلى حزيران 2006 ما وصل إلى 2037 مهمة، وحلّقت لمدة 33833 ساعة، ومسحت 18490 هدفًا، وشاركت في 242 غارة منفصلة. وحتى مع هذا المجهود الهائل، ما يزال هناك طلب على المزيد (سينجر،2010: 59).

وإلى جانب «بريديتور» هناك الطائرة «ريفين» التي لا يزيد طولها على 38 بوصة، وتزن أربعة أرطال. ومن باب المفارقة أنّ الجنود يطلقون هذه الطائرة الصغيرة باستخدام الحركة نفسها من أعلى الكتف التي كان المحاربون الرومان يستخدمونها في الحرب قبل ألفي عام، مع فارق أنهم يقذفون روبوتًا بدلًا من الرمح القديم، ثم تنطلق «ريفين» حيث يمكنها التحليق مدة 90 دقيقة على ارتفاع نحو 400 قدم حاملة ثلاث كاميرات، تعمل واحدة منها بالأشعة تحت الحمراء، والجنود يحبونها لأنها تمكنهم من التحديق من أعلى التل أو مجمع البنايات التالي، ويحصلون على طائراتهم التجسسية الخاصة بدلًا من الاضطرار إلى استجداء الدعم (Justin، 2003: 12).

أمّا روسيا فتستخدم أنظمة الطائرات دون طيار، والقنابل والصواريخ الموجهة، ومنظومة الملاحة الفضائية «غلوناس» pechla-1T، حيث ظهرت تلك الطائرة دون طيار لأول مرة فوق إدلب السورية في شهر آب عام 2014، وهي تختص بمهام المراقبة والاستطلاع وتزويد وحدات المشاة والمدفعية بإحداثيات الكتل المعادية، كما تستخدم القنابل والصواريخ الموجهة، حيث أعلن المتحدث باسم وزارة الدفاع الروسية «إيغور كليموف» أن القوات الجوية الروسية تستعمل في غاراتها على مواقع الإرهابيين في سورية صواريخ موجهة بالليزر عالية الدقة، ومن تلك الصواريخ «إكس 29 إل» التي تحتوي على رؤوس ليزرية، وعند إطلاق الصاروخ يحدد الطيار الهدف بأشعة الليزر، ويمكنه مواصلة المناورة. وأوضح كليموف أنّ الصاروخ لا يبتعد عن هدفه أكثر من مترين، ويبلغ وزنه 500 كلغ، ويصيب الأهداف الدقيقة ويحتوي على مواد انشطارية شديدة الانفجار، وأضاف أنّ هذه الصواريخ تطلق من القاذفات «سو-24»، و«سو-34» قنبلة «كاب 500 إس» مجهزة بنظام توجيه الأقمار الصناعية والرؤوس الحربية شديدة الانفجار، وهي تنتمي إلى الأسلحة عالية الدقة، وتعمل من خلال مبدأ «أسقط وانسَ»، وهي مصممة للاشتباك مع الأهداف البرية والبحرية الثابتة مثل المخازن والسفن الراسية ليلًا ونهارًا وفي كلّ الأحوال الجوية (هيرش، 2016: 14).

وقد تم استخدام الذكاء الاصطناعي أيضًا في مواجهة العمليات الإرهابية داخل حدود الدولة، فقد صنعت شركة «سكيوريكس» الأمريكية - مثلًا - منظومات لصالح قيادة العمليات الخاصة الأمريكية ووكالة مشروعات

البحوث المتقدمة التابعة لوزارة الدفاع، بوصفها جزءًا من «برنامج الهوية البشرية من بعيد» الخاص بالوكالة، والذي يمكنه مسح الوجوه والتعرف عليها من بعد يصل إلى مئتي قدم. وستجمع برامج أخرى الذكاء الاصطناعي وأحدث البحوث في مجال علم المحاكاة الطبيعية، فقد تتحرى على سبيل المثال وجود شخص ما يخبئ شيئًا تحت ملابسه، قنبلة مثلًا، وذلك بتحليل كيفية تغير طريقة مشيته.

ويتم في مجال عمليات تصفية قيادات التنظيمات الإرهابية استخدام الأقمار الصناعية وعمليات التنصت الإلكتروني لتحديد مواقع اختباء أو إقامة هذه القيادات، ولعلّ المثال الأبرز على ذلك هو عملية اغتيال زعيم القاعدة أسامة بن لادن، فقد كشفت الوثائق أنّ الأقمار الصناعية التي يديرها مكتب الاستخبارات القومي، أجرت أكثر من 387 عملية لجمع صور عالية الدقة وصور ما تحت الأشعة الحمراء لمجمع «أبوت آباد» الباكستاني الذي كان يختبئ فيه بن لادن في الشهر الذي سبق العملية، وكانت هذه الصور والمعلومات على درجة كبيرة جدًا من الأهمية للتحضير لعملية الاغتيال، واتخاذ قرار الموافقة على تنفيذ العملية.

الفصل الثالث

حرب الفضاء الإلكتروني

مع الاستخدام الكثيف لتكنولوجيا المعلومات وارتباطها الوثيق بمفهوم الحرب، أصبح الفضاء الإلكتروني فاعلًا ومؤثرًا في النظام الدولي والعلاقات الدولية، وأصبحت المصالح الاستراتيجية ذات الطبيعة الإلكترونية عرضة للتهديد بتحول ساحة الصراع والحروب الدولية إلى الفضاء الإلكتروني، الأمر الذي جعل قضية أمن الفضاء الإلكتروني تلقى اهتمامًا متصاعدًا على أجندة الأمن الدولي، الذي امتد من حماية الدولة من التعرض لهجوم عسكري إلى حماية المنشآت الحيوية للبنية التحتية من التعرض لأعمال هجومية باستخدام محكم لتكنولوجيا الاتصال والمعلومات. وأصبحت قضية أمن الفضاء الإلكتروني من أعلى مستويات استراتيجية الأمن القومي للعديد من الدول المتقدمة للعمل على الحيلولة دون تعرض بنيتها التحتية الحيوية للخطر والتهديد.

وقد أصبحت إمكانية إصابة الآلاف أو الملايين من الحواسيب بفيروس ما في ساعات قليلة أمرًا محتملًا، بحيث يتحول كلٌّ منها إلى محطة لبث الفيروس المعني، يجعل قدرتها على الإضرار في ارتفاع مُطّرِد، وبذلك فإن قدرة عدد صغير من الأفراد على تكبيد قوة عظمى خسائر هائلة يدفع بمفهوم الصراع غير المتناظر إلى أقصى درجاته.

وقد زادت حالة الانكشاف الأمني للدول نتيجة لاعتمادها المتزايد على الفضاء الإلكتروني في مختلف النشاطات مثل برامج الحكومة

الإلكترونية، التي تصبح عرضة للاختراق والهجوم بالفيروسات وسرقة المعلومات وإتلافها.

لقد كان المفهوم العام لحرب الفضاء الإلكتروني مقصورًا على عمليات التشويش على أنظمة الرادار وأجهزة الإنذار، بينما يكشف الواقع الحالي عن دخول شبكات الاتصال والمعلومات إلى بنية ومجال الاستخدامات الحربية. وبالإضافة إلى ذلك كان مسمى الحرب يعني استخدام جيوش نظامية وتحديد ميدان قتال محدد، أمّا هجمات حرب الفضاء الإلكتروني فإن ميدان القتال فيها مفتوح لأنها تتحرك عبر شبكات المعلومات والاتصال المتعدية للحدود الدولية.

• ماهية حرب الفضاء الإلكتروني

لقد استُخدِم مصطلح (Cyberspace) للتعبير عن الإنترنت في عام 1991، وأصبح هذا المفهوم أوسع وأشمل من الإنترنت ليضم جميع الاتصالات والشبكات وقواعد البيانات ومصادر المعلومات، وأصبحت بنية النظام الإلكتروني تعني المكان الذي لا يُعَدّ جزءًا من العالم المادي أو الطبيعي، حيث إنها ذات طبيعة افتراضية رقمية إلكترونية تتحرك في بيئة إلكترونية حيوية تعمل من خلال خطوط الهاتف والكابلات الاتصالية والألياف البصرية والموجات الكهرومغناطيسية. ويمكن وصف العالم الإلكتروني بأنه عبارة عن شبكات الكمبيوتر والاتصالات الإلكترونية،

وهو عبارة عن شبكة كمبيوتر خيالية تحتوي على كم هائل من المعلومات التي يمكن الحصول عليها لتحقيق الثروة والسلطة، بحيث يصبح استخدامه محل نزاع بين الدول، ويعدّ اختراقه تهديدًا صريحًا لأمن ومصالح الدول أيضًا.

ولذلك تمت إعادة التفكير دوليًا في مفهوم الأمن الذي امتد من حماية الدولة من التعرض للهجوم العسكري إلى حماية المنشآت الحيوية للبنية التحتية من التعرض لأعمال عدائية من خلال استخدام تكنولوجيا الاتصال والمعلومات، وأصبحت قضية أمن الفضاء الإلكتروني تدخل في استراتيجيات الأمن القومي للعديد من الدول المتقدمة للعمل على الحيلولة دون تعرض بيئتها التحتية الحيوية للخطر (Tim، 2000: 175).

وقد أصبحت حرب الفضاء الإلكتروني بديلًا عن الحرب المباشرة بين الدول، وباتت القدرة على القيام بهجمات إلكترونية أداة سيطرة ونفوذ استراتيجية بالغة الأهمية سواء في وقت السلم أم في وقت الحرب، بسبب زيادة علاقة الفضاء الإلكتروني بعمل المنشآت الحيوية المدنية والعسكرية للدول، مما أدى إلى إمكانية تعرضها لهجمات إلكترونية تستهدف الشبكة كوسيط وحامل للخدمات أو تشل عمل أنظمتها المعلوماتية، مما يعرقل قدرتها على القيام بوظائفها.

وأدى ذلك إلى دخول المجتمع الدولي في مرحلة جديدة تلعب فيها هجمات الفضاء الإلكتروني دورًا أساسيًا في تعظيم القوة أو الاستحواذ

على عناصرها الأساسية، وأصبح التفوق في مجال الفضاء الإلكتروني عنصرًا حيويًا في تنفيذ عمليات ذات فاعلية على الأرض، وفي البحر والجو والفضاء من خلال نظم التحكم والسيطرة (Arsenio، 1996: 66).

وقد زادت حالة الانكشاف الأمني للدول نتيجة لاعتمادها المتزايد على الفضاء الإلكتروني في مختلف النشاطات مثل برامج الحكومة الإلكترونية التي تصبح عرضة للاختراق والهجوم بالفيروسات وسرقة المعلومات وإتلافها (Gabriel، 2006: 243)، ووقعت حالة الانكشاف الأمني هذه بفعل ظهور الحواسيب والشبكات والذكاء الاصطناعي، وكلّها مترابطة على مستوى الكوكب كلّه. وتقوم قيادة الحرب اليوم على مجموعة اتصالية رقمية لا مثيل لها، تتكون من شبكات كثيفة للرصد والإعلام والاتصال والتحديد الجغرافي والتنصت الإلكتروني والتشويش وفك الرموز والتحليل والمحاكاة.

وبالنسبة لساحة حرب الفضاء الإلكتروني نجد أنّ هذه الساحة هي جهاز الحاسوب المحمول الذي يرتبط بكابل يربطه بأجهزة الخوادم. وقد أصبح الفضاء الإلكتروني اليوم ساحة حرب تشهد كثيرًا من المعارك الحاسمة في القرن الحادي والعشرين. وما يجعل من هذه الأماكن ساحة لقتال قوات حرب الفضاء الإلكتروني هو أنّ قوات حرب الفضاء الإلكتروني تستطيع أن تدخل في قلب هذه الشبكات وتسيطر عليها أو تدمرها، وإذا استولت على شبكة ما أمكنها أن تسرق كلّ معلوماتها، أو

ترسل إليها تعليمات بتحويل الأموال أو تسريب النفط أو إطلاق الغاز أو تفجير المولدات أو إخراج القطارات عن قضبانها أو صدم الطائرات، ويمكنها أيضًا إرسال كتيبة لتقع في كمين، أو تفجير قذيفة في المكان الخطأ، أو إخراج الأقمار الصناعية عن مداراتها لتذهب على غير هدى في الفضاء السحيق، أو إيقاف رحلات الخطوط الجوية تمامًا. وهذه الأمور ليست افتراضات متخيَّلَة، فقد حدثت وقائع مثلها على سبيل التجريب أحيانًا، وعلى سبيل حرب الفضاء الإلكتروني أحيانًا أخرى. فالمعلومات التي تتعامل معها شبكات الحاسوب والتي تدير المرافق ووسائل المواصلات والمصارف يمكن استغلالها ومهاجمتها في ثوان، ولا تستطيع الجيوش والأساطيل الدفاع عنها لأنها تقع في المجال الرقمي للفضاء الإلكتروني.

• تعريف حرب الفضاء الإلكتروني

من الصعب تقديم تعريف محدد للفضاء الإلكتروني، فهناك العديد من الآراء المتفاوتة حول الطابع الذي يحدد الفضاء الإلكتروني، فهناك من يرى أنه ذو طابع افتراضي، حيث يُعرَّف بأنه «تلك البيئة الافتراضية التي تعمل فيها المعلومات الإلكترونية، والتي تتصل عن طريق شبكات الكمبيوتر»، ويعرفه آخرون بأنه «المجال الذي يتميز باستخدام الإلكترونيات لتخزين وتعديل وتغيير البيانات عن طريق النظم المرتبطة

والمتصلة بالبيئة التحتية الطبيعية، ومن ثم فإنه يشمل عملية الاندماج ما بين الإنترنت والمحمول وأجهزة الاتصالات والاقمار الصناعية».

ويمكن اعتبار الفضاء الإلكتروني مجموعة من شبكات الحاسوب في العالم وكلّ ما ترتبط به وتتحكم فيه. ويشمل الفضاء الإلكتروني الإنترنت إلى جانب العديد من شبكات الحاسوب السرية الأخرى التي لا يمكن الوصول إليها عبر الإنترنت، وبعض هذه الشبكات الخاصة يشبه شبكة الإنترنت تمامًا لكنّها منفصلة عنها نظريًا على الأقل، كما يشمل الفضاء الإلكتروني الشبكات التجارية التي تقوم بمهام مُعيّنة من قبيل إرسال البيانات الخاصة بالتدفقات المالية والمعاملات في الأسواق المالية ومعاملات البطاقات الائتمانية، وبعض الشبكات هي نفسها نظام للتحكم، بمعنى أنها هي التي تسمح للأجهزة بمخاطبة غيرها من الأجهزة مثل لوحات التحكم التي تخاطب البنى التحتية الاستراتيجية كالمضخات ومولدات الطاقة والكهرباء. وهناك ثلاثة أمور في عالم الفضاء الإلكتروني تجعل من الحرب الإلكترونية أمرًا ممكنًا وهي:

1. وجود ثغرات في تصميم الإنترنت.
2. وجود ثغرات في المعدات والبرمجيات.
3. الاتجاه لتوصيل المزيد من الأجهزة والقطاعات على شبكات الفضاء الإلكتروني.

أما مصطلح حرب الفضاء الإلكتروني فيشير إلى الإجراءات التي تتخذها أي دولة لاختراق أجهزة الحاسوب والشبكات الخاصة بدولة أخرى لغرض السيطرة عليها أو التحكم بها أو إتلافها أو تعطيلها عن العمل من خلال إرسال رسائل مكتوبة باللغة الرقمية الثنائية المكونة من رقمي (0-1).

ويستخدم بعض الخبراء تعريفًا ضيقًا لحرب الفضاء الإلكتروني، فهي حرب غير دموية بين الدول تشمل فقط الصراع الإلكتروني في الفضاء السيبراني، ولكنّ هذا التعريف يتجاهل الترابط المهم بين الطبقات المادية والافتراضية للفضاء الإلكتروني، فحرب الفضاء الإلكتروني هي عمل عدائي في الفضاء الإلكتروني، تؤدي التأثيرات المترتبة عليه إلى تضخيم العنف المادي أو تعادله (ناي، 2005، 1). لذلك كان لا بدّ للدول من تعزيز دفاعاتها ضد خطر التعرض للهجمات الإلكترونية، والاتجاه إلى التحول من اتخاذ إجراءات وقائية ذات طابع دفاعي إلى الاتجاه نحو تبني سياسات هجومية، ويحمل ذلك في طياته مخاطر عسكرة الفضاء الإلكتروني، وخصوصًا أنّ القدرة على السيطرة على هذا النوع من الأسلحة ضئيلة بالمقارنة مع الأسلحة التقليدية. وهناك مسألة صعوبة تحديد الأسلحة التي يمتلكها الآخرون، ومن ثم يصبح لدى المجتمع الدولي قدرة سريعة على التدخل لاحتواء التقدم في مجال هذه الأسلحة (عبد الصادق، 2012: 33).

وقد تشجع طبيعة حرب الفضاء الإلكتروني على المبادرة إلى شنّ الهجوم، وأكثر الأهداف المحتملة التي تتعرض لها هي الأهداف المدنية، وبالإضافة إلى ذلك فإنّ السرعة التي تتحرك بها والتي يمكن من خلالها ضرب آلاف الأهداف في أي مكان بالعالم، قد تؤدي إلى نشوب الأزمات الشديدة، فالقوة التي حالت دون وقوع الحرب النووية هي قوة الردع، لكنها لا تجدي في مجال حرب الفضاء الإلكتروني (كلارك، 2012: 90).

وقد أدى تعدد أنماط استخدام الفضاء الإلكتروني وتداخلها ما بين ما هو مدني وما هو عسكري إلى عدم وجود إجماع على تعريف محدد ودقيق لمفهوم حرب الفضاء الإلكتروني، فهناك من عرّفها بأنها أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها، بينما عرّفها آخرون بأنها مفهوم يشير إلى نزاع يحدث في الفضاء الإلكتروني يكون له طابع دولي.

لا يوجد حتى اليوم فهم كامل للتهديدات الإلكترونية، وذلك بسبب حداثة هذه التهديدات والتطور السريع لها، وبسبب النقص في المصطلحات الفنية المُتفَق عليها لوصف هذه التهديدات. فالأمن الإلكتروني غالبًا ما يجري تبسيطه كحماية الشبكات وأنظمة البيانات، لكنّ زيادة عدد الهجمات على الشبكات المالية والحكومية والعسكرية، جعل من الأمن الإلكتروني أسبقية في مجال الأمن (Michael، 2009: 30).

وتتأثر حرب الفضاء الإلكتروني بما يحدث في البيئات الأخرى من نزاعات بين الجماعات والأفراد، وصراعات بين الدول. ولأنّ الحروب الفعلية تستعمل شتى أنواع أسلحة التدمير فإنّها لم تتوانَ في استخدام الفضاء الإلكتروني لما له من تأثير أمني وعسكري (عبد الصادق، 2012: 29).

يغطي مصطلح حرب الفضاء الإلكتروني مجموعة واسعة من الإجراءات، تتراوح بين المِجسّات البسيطة المستخدمة لمحو المواقع على شبكة الإنترنت، والحرمان من الخدمة، والتجسس والتدمير، ويُستخدَم على نحو مماثل لتغطية مجموعة واسعة من السلوكيات، وهو يعكس تعريفات قاموسية للحرب تتراوح بين الصراع المسلح والتسابق العدائي (Joseph، 2012: 2).

• خصائص حرب الفضاء الإلكتروني

يُعَدّ الفضاء الإلكتروني مجالًا عامًا وسوقًا مفتوحة، وتدلل على وجوده شبكة من التواصل والعلاقات بين من يستخدمونه ويتفاعلون معه، مع انتقال كافة مجالات الحياة من إعلام وصحة وتعليم وحكومة واقتصاد وسياسة إلى الفضاء الإلكتروني. وإلى جانب ذلك أصبح الفضاء الإلكتروني وسيطًا ووسيلة لشنّ الهجوم وتنفيذ الاعمال العدائية بين الخصوم كغيره من مجالات الجو والفضاء والبحر، وقد أصبح بذلك

وسيطًا جديدًا للصراع. ويحوي الفضاء الإلكتروني كمًّا هائلًا ومتسعًا من الشبكات ونظم المعلومات نتيجة اتصاله وتداخله مع الفضاء الخارجي والأقمار الصناعية.

والفضاء الإلكتروني لا حدود له، حيث يتشارك كل الفاعلين بما فيهم الدول في مجالاته من الاستخدام الشخصي إلى البرامج الاقتصادية والتطبيقات العسكرية، وكلّها تعتمد على الفضاء الإلكتروني. وعلى العكس من التهديدات التقليدية الملموسة التي يمكن التنبؤ بها، فإنّ تهديدات الفضاء الإلكتروني يمكن أن تأخذ شكلًا ومصدرًا افتراضيًا، وتفرض أخطارًا لا يمكن التنبؤ بها. ويمكن القول إنّ أهم خصائص حرب الفضاء الإلكتروني هي:

أولًا: إنّ حرب الفضاء حقيقة واقعة، ويلاحَظ أن الولايات المتحدة وبعض الدول الأخرى قادرة على أن تشنّ من حروب الفضاء الإلكتروني ما يدمر غيرها من الدول الحديثة.

ثانيًا: إنّ حرب الفضاء الإلكتروني تحدث بسرعة الضوء، فعندما تتدفق فوتونات الحزم المهاجمة عبر الألياف الضوئية، يكون الوقت المستغرق لشنّ الهجمة وتأثيرها سريعًا جداً يكاد يتعذر قياسه، مما يخلق المخاطر أمام صُنّاع القرار في أثناء الأزمات.

ثالثًا: إنّ حرب الفضاء الإلكتروني هي حرب عالمية الطابع، وفي نطاق أو صراع يستشري فيه العدوان الإلكتروني على مستوى العالم، لأنّ

أجهزة الحاسوب والأجهزة الخادمة المختَرَقَة خفية، وكذلك الأجهزة التي تمت السيطرة عليها في شتى أنحاء العالم، إذ سرعان ما تنضم إلى الهجمات فتجرّ بلاد كثيرة إلى الصراع سريعًا.

رابعًا: إنّ حرب الفضاء الإلكتروني لا تحتاج إلى ساحات المعارك التقليدية، فالأنظمة المختلفة التي يعتمد عليها الناس - من المصارف والمطارات والطائرات وبطاقات الائتمان وشبكات الكهرباء والطاقة والبريد، وصولًا إلى رادارات الدفاع الجوي وأنظمة الصواريخ -يمكن الوصول إليها عبر الفضاء الإلكتروني والسيطرة عليها سريعًا أو تعطيلها دون الحاجة إلى دحر الدفاعات التقليدية للدول.

خامسًا: لقد بدأ عصر حرب الفضاء الإلكتروني، وصارت الدول تتحسب لوقوع الهجمات الإلكترونية، فبدأت تُعِدّ ساحة المعركة وذلك بأن يحاول كلٌّ منها اختراق شبكات الدول وزرع ثغرات التسلل والقنابل المنطقية، وكلّ هذا يتم في وقت السلم. وهذا الطابع لحرب الفضاء الإلكتروني يطمس الحدود الفاصلة بين السلم والحرب، ويخلق بعدًا جديدًا في حالة انعدام الاستقرار.

• عوامل قياس القوة في مجال حرب الفضاء الإلكتروني

تصاعدت مخاطر العلاقة بين الأمن والتكنولوجيا في المشهد الدولي، وبقدر ما أسهم الفضاء الإلكتروني في بروز مناخ إيجابية الاستخدامات

المدنية التي تحمل أهمية متعددة الأوجه، فإنّها أتاحت الفرص كذلك للاستخدام غير السلمي ومظاهره التي منها ما هو ذو طابع تخريبي، مثل الهجمات والحروب الإلكترونية، ومنها ما هو ذو طابع مرن ومنخفض الشدة، كالتجسس وحرب المعلومات من جانب الاستخبارات الدولية من أجل دعم أنشطتها السرية في جمع المعلومات من مناطق الاستهداف، ومعرفة توجهات الرأي العام في الدول المختلفة، والإحاطة بتوجهات القادة والزعماء والنخب، ودوائر صنع القرار القريبة (عبد الصادق، 2014: 166). وتُعَدّ أساليب حرب المعلومات والقرصنة الإلكترونية واستخبارات المصادر المفتوحة من أهم أدوات حرب الفضاء الإلكتروني.

يمكن استخدام أسلحة حرب الفضاء الإلكتروني بسرعة وسهولة ودون الفهم الكامل للتفاقم التصاعدي الذي قد ينجم عنها، فعلى الرغم من أنّ الحرب قد تبدأ في الفضاء الإلكتروني بلا جنود وبلا إراقة دماء، إلّا أنها لا تظل كذلك طويلًا في بعض الأحيان، فقيام بعض الدول بزراعة الأسلحة الإلكترونية في شبكات البنية التحتية في غيرها من الدول يجعل فتيل الحرب سهل الاشتعال أكثر من أي وقت مضى في تاريخ الحروب. وبالنسبة لأثر أسلحة الفضاء الإلكتروني، فإنّه يقلّ عن أثر الأسلحة النووية، ولكنّ استعمالها في ظروف معينة قد يُحدِث أضرارًا فادحة، وقد

يشعل فتيل حرب واسعة. ويمكن قياس القوة في مجال حرب الفضاء الإلكتروني من خلال تقييم ثلاثة عوامل (كلارك، 2012: 249):

1. الهجوم: أي قدرة الدولة على شنّ هجمات إلكترونية على الدول الأخرى.
2. القدرة على الدفاع: ويعني قياس قدرة الدولة على اتخاذ إجراءات عند تعرضها للعدوان لصدّ هجمة أو تخفيف آثارها.
3. الاعتماد: ويعني مدى اتصال الدولة بالإنترنت، واعتمادها على الشبكات والأنظمة التي قد تكون عرضة للأخطار في حالة وقوع حرب إلكترونية.

• أمن المعلومات الإلكترونية

يرى عدد من المتخصصين بعلوم الاقتصاد وتكنولوجيا المعلومات والعلوم الاجتماعية في العالم، بأن مفهوم أمن المعلومات الإلكترونية قد ظهر في العصر الجديد (عصر الثورة المعلوماتية) نتيجة التحول الذي طرأ على المجتمعات البشرية، بحيث انتقلت من مجتمعات صناعية إلى مجتمعات معلوماتية، تعتمد في إدارة شؤونها الحياتية على التكنولوجيا الرقمية والإلكترونية، والاقتصاد الرقمي والمعلوماتي، واقتصاديات المعرفة.

أيقنت حكومات العالم في عصرنا الإلكتروني أنّ اعتمادها على الأداء التقليدي لوزاراتها وأركانها الحكومية في ظل هذا التنامي الكبير للوسائل

التقنية والرقمية قد يصيبها بالهرم والشيخوخة الإدارية والقيادية، ويوسع من الفجوة الموجودة بينها وبين جمهورها، لذلك لجأت هذه الحكومات إلى اللحاق بركب الحضارة الرقمية والإلكترونية، لتعزيز عمل مؤسساتها الحكومية، وحوسبة قطاعاتها الخدماتية بشكل تقني وإلكتروني، حيث أصبح هذا التحول التكنولوجي معيارًا تقاس به درجة تقدم الدول، ومقياسا لمدى الرضى الذي تحظى به من قبل جماهيرها.

وفي خضم هذا الوعي التقني والمعلوماتي والإلكتروني الذي أوجدته تكنولوجيا المعلومات في عصرنا الحاضر، تحولت البشرية بأسرها إلى منتِجة ومتلقِية ومستخدِمة لوسائل الاتصال الحديثة بشكل كبير، وعملت بدورها على إحلال الأنظمة الإلكترونية الرقمية من هواتف محمولة وحواسيب متطورة، وشبكات تكنولوجية متصلة بالإنترنت، وأنظمة للتشغيل ذات طاقة عالية، مكّنت الإنسان من الاطّلاع على عالمه الخارجي بشكل أكثر وضوحًا ونقاء (شيخاني، 2010: 435).

وعلى الرغم من الصورة الباهرة التي رسمتها تكنولوجيا المعلومات للإنسانية، ومحاسن الثورة المعلوماتية التي غمرت البشرية في عصرنا الحالي، فإنّها أدخلت دول العالم في هاجس أمني قوي، وخصوصًا أنّ هذه الدول قامت بوضع مدخراتها القومية على شكل معلومات رقمية عبر فضاء مذاب الخصوصية، وضعيف الأمن- لبعض الدول- وفائق السرعة، وزنبقي الشكل، مما زاد من الفجوة المعلوماتية القومية بين الدول.

ويمكن بالتالي تعريف أمن المعلومات الإلكترونية بأنّه العلم الذي يبحث في نظريات واستراتيجيات ووسائل حماية المعلومات الإلكترونية من المخاطر والأخطار التي تهددها، واتخاذ الإجراءات والأدوات التكنولوجية لحماية تلك المعلومات من أية أنشطة اعتدائية ضارة، قد تؤثر على فحواها وجوهرها (إبراهيم، 2008: 28).

ويشير الأمن السيبراني إلى مجموعة التقنيات والعمليات والممارسات المصممة لحماية الشبكات والأجهزة والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به، وقد يُشار أيضًا إلى الأمن السيبراني على أنه أمن تكنولوجيا المعلومات.

ويُعَدّ الأمن السيبراني مهمًا لأنّ المنظمات الحكومية والعسكرية والشركات والمؤسسات المالية والطبية تجمع وتعالج وتُخزّن كميات غير مسبوقة من البيانات على أجهزة الكمبيوتر والأجهزة الأخرى، يمكن أن يكون جزء كبير منها معلومات حساسة، سواء كانت ملكية فكرية أم بيانات مالية أم معلومات شخصية أو أنواع أخرى من البيانات التي يمكن أن يؤدي الوصول غير المصرح به إليها أو التعرض لها إلى نتائج سلبية.

تنقل المؤسسات بيانات حساسة عبر الشبكات وإلى أجهزة أخرى أثناء ممارسة الأعمال، ويصف الأمن السيبراني الانضباط المخصص لحماية تلك المعلومات والأنظمة المستخدمة في معالجتها أو تخزينها، مع تزايد حجم وتعقيد الهجمات السيبرانية. تحتاج الشركات والمنظمات - وخصوصًا تلك المكلفة بحماية المعلومات المتعلقة بالأمن القومي أو

الصحة أو السجلات المالية - إلى اتخاذ خطوات لحماية أعمالها الحساسة ومعلومات الموظفين.

ومن أجل أمن سيبراني فعال، تحتاج المنظمة إلى تنسيق جهودها عبر نظام المعلومات بأكمله. وتشمل عناصر الإنترنت كلّ ما يلي:

- أمن الشبكة: عملية حماية الشبكة من المستخدمين غير المرغوب فيهم ومن الهجمات والاقتحامات.
- أمان التطبيق: تتطلب التطبيقات تحديثات واختبارات مستمرة لضمان أمان هذه البرامج من الهجمات.
- أمان نقطة النهاية: يُعَدّ الوصول عن بُعد جزءًا ضروريًا من العمل، ولكن يمكن أن يكون أيضًا نقطة ضعف للبيانات، وأمان نقطة النهاية هو عملية حماية الوصول عن بعد إلى شبكة الشركة.
- أمان البيانات: البيانات داخل الشبكات والتطبيقات، وحماية معلومات الشركة والعملاء طبقة منفصلة من الأمان.
- إدارة الهوية: هي - بشكل أساسي - عملية لفهم الوصول لكلّ فرد في المنظمة.
- أمن قواعد البيانات والبنية التحتية: كل شيء في الشبكة يتضمن قواعد البيانات والمعدات المادية، وحماية هذه الأجهزة مهمة بالقدر نفسه.

- أمان السحابة: توجد العديد من الملفات في بيئات رقمية أو في «السحابة». وتمثل حماية البيانات في بيئة الإنترنت بنسبة 100٪ قدرًا كبيرًا من التحديات.
- أمان الهاتف المحمول: تتضمن الهواتف المحمولة والأجهزة اللوحية كلّ نوع من التحديات الأمنية في حد ذاتها.
- تخطيط التعافي من الكوارث/ استمرارية العمل: في حالة حدوث اختراق، يجب الكوارث الطبيعية أو غيرها من الأحداث، ويجب أن تستمر الأعمال، ولهذا ستحتاج حماية هذه البيانات إلى تخطيط مسبق.
- تدريب المستخدم النهائي: قد يكون المستخدمون موظفين يصلون إلى الشبكة أو عملاء يقومون بتسجيل الدخول إلى تطبيق الشركة، ولذلك يُعَدّ تعليم العادات الجيدة (تغيير كلمة المرور، والمصادقة الثنائية، وما إلى ذلك) جزءًا مهمًا من الأمن السيبراني.

إن أصعب تحدٍّ في الأمن السيبراني هو الطبيعة المتطورة للمخاطر الأمنية نفسها. وقد ركزت المنظمات والحكومات - تقليديًا - معظم موارد الأمن السيبراني على أمن المحيط لحماية مكونات النظام الأكثر أهمية والدفاع عنها. ويُعَدّ هذا النهج اليوم غير كاف، حيث تتقدم التهديدات وتتغير بسرعة أكبر من قدرة المنظمات والحكومات على مواكبتها. ونتيجة لذلك، تعزز المنظمات الاستشارية مناهج أكثر استباقية وتكيفية للأمن السيبراني.

ولإدارة موضوع الأمن السيبراني لا بدّ من اتباع نهج (من أعلى إلى أسفل)، حيث تتولى إدارة المنظمة أو الحكومة المسؤولية في تحديد أولويات إدارة الأمن السيبراني في جميع ممارسات الأعمال، ويجب أن تكون مستعدة للاستجابة للحادث السيبراني الحتمي، واستعادة العمليات العادية، وضمان حماية الأصول والبنى التحتية.

وقد قامت الولايات المتحدة الأمريكية في هذا الصدد بإنشاء ما يُسمّى (المركز الوطني لتطبيقات الحوسبة الفائقة NCSA)، وتركزت مبادئه التوجيهية لإجراء تقييمات المخاطر السيبرانية على ثلاثة مجالات رئيسية هي: تحديد «جواهر التاج» في المؤسسة، أو المعلومات الأكثر قيمة التي تتطلب الحماية، وتحديد التهديدات والمخاطر التي تواجه تلك المعلومات، وتحديد الضرر الذي ستتعرض له المنظمة أو الحكومة في حالة فقدان البيانات أو كشفها بشكل خاطئ.

ويجب أن تأخذ تقييمات مخاطر الإنترنت أيضًا في الاعتبار أي لوائح تؤثر على طريقة جمع البيانات وتخزينها وتأمينها، ولا بدّ -بعد تقييم مخاطر الإنترنت- من التخطيط للتخفيف من مخاطر الإنترنت، وحماية «جواهر التاج»، واكتشاف الحوادث الأمنية والاستجابة لها بشكل فعال. ويجب أن يشتمل التخطيط على كلّ العمليات والتقنيات المطلوبة لبناء برنامج قوي للأمن السيبراني في مجال دائم التطور، كما يجب تطوير أفضل ممارسات الأمن السيبراني لاستيعاب الهجمات المتزايدة التعقيد التي يقوم بها المهاجمون.

ويوفر الجمع بين إجراءات الأمان السيبراني السليمة وقاعدة الموظفين المتعلمين والمثقفين أفضل دفاع ضد مجرمي الإنترنت الذين يحاولون الوصول إلى البيانات الحساسة، على الرغم من أنها قد تبدو مهمة صعبة.

وقد غدت متلازمة أمن المعلومات الإلكترونية والأمن القومي ضرورة قومية وجب على جميع الدول احتضانها، والعمل على إدراجها ضمن سياساتها العامة، فغالبية المحتوى المعلوماتي لدول العالم أصبح متوفرًا على الشبكات العالمية، حيث أصبحت إمكانية الاطلاع عليها متاحة عبر استخدام التقنيات الحديثة والذكية. ولذلك أصبح لكلّ بعد أو محتوى أو مجال أمني قومي لأي دولة في العالم وجه معلوماتي ورقم ينبغي الحفاظ عليه، وهذه الأبعاد والمجالات أهمها:

1. الأمن القومي العسكري: تعمل غالبية الابتكارات العسكرية والتسليحية في وقتنا الحاضر من خلال ربطها بوسائل الاتصال الحديثة، وشبكة الإنترنت، وقواعد البيانات وأنظمة المعلومات العسكرية والحربية التي تُمَكّن مستخدميها من التحكم بها عن بعد، ويُعَدّ المحتوى المعلوماتي الرقمي العسكري من أخطر الأبعاد تأثيرًا على الأمن القومي لأي دولة في العالم، نظرًا لحساسية ما يحتويه من معلومات رقمية وإلكترونية عن الجوانب العسكرية والتسليحية للدول.

2. الأمن القومي الاجتماعي: يُعَدّ هذا البعد الأمني وجهًا تعريفيًا عن البيانات ونظم المعلومات المتخصصة للتعامل مع الحالة الاجتماعية للدولة ككلّ، كالدراسات الإحصائية والسكانية وغيرها، بحيث تشكل في حال الاطلاع عليها بشكل غير قانوني تهديدًا لسلامة المجتمع بأسره.
3. الأمن القومي السياسي: يتلخص هذا المحتوى الأمني بالبيانات الرقمية، والمعلومات الإلكترونية التي تخص الأحزاب في الدولة، إضافة إلى المعلومات التي تتعلق بالبرلمانات، ورئاسة الدولة، وأجهزتها السيادية، وهي معلومات حساسة قد تؤدي إلى حروب أهلية في حال العبث بها.
4. الأمن القومي الفكري والثقافي والإعلامي: يشكل هذا البعد ذروة الإنتاج الفكري لأي دولة في العالم، وهي معلومات ذات طابع جماعي وفردي على حد سواء، وهي تعتمد على وسائل الاعلام الحديثة التي تساهم في رفع أو خفض مظاهر الأمن القومي لأي دولة، كالمظهر المادي المتعلق باستقرار المواطنين، والذي له علاقة مباشرة بخفض أو رفع الهواجس الأمنية لدى الدولة.
5. الأمن القومي العلمي والبحثي: يتعلق هذا المحتوى الأمني والقومي بالبيانات والمعلومات الخاصة بالمؤسسات البحثية والعلمية والجامعات، وهي تشكل ثروة قومية مستقبلية تحوي العديد من

الاكتشافات وبراءات الاختراع المُعرَّضة للسرقة أو القرصنة الإلكترونية.

6. الأمن القومي للجهاز الإداري الحكومي: يتلخص هذا الجانب الأمني والقومي بالخدمات الإلكترونية المقدمة للجماهير، والمتعلقة بأعمال الحكومة الإلكترونية. وتقوم هذه الخدمات على عنصر الثقة المتبادلة بين الحكومة ومواطنيها، ويعني ذلك أنّه في حال تعرض هذه الأعمال للقرصنة، فإنّ الحكومة تفقد مصداقيتها من قبل مواطنيها، وخصوصًا في الدول المتقدمة إلكترونيًا.
7. الأمن القومي الاقتصادي: هو أكثر القطاعات الأمنية والقومية عرضة للهجمات الإلكترونية، نظرًا لتحول اقتصاديات العالم إلى كيانات اقتصادية معرفية معتمدة على المعلومات الرقمية، كالبنوك والبورصات وغيرها، التي تشكل في حال التعرض لها خسائر اقتصادية وقومية هائلة.

● حرب المعلومات

لا بدّ لنا – عند الحديث عن أمن المعلومات الإلكترونية – من تسليط الضوء على مصطلح (حرب المعلومات) الذي ظلّ موضوع نقاش حتى منتصف التسعينات، فكانت حرب المعلومات تشير إلى مجموعة من البرامج الخاصة بالدفاع والأمن القومي، أو إلى برامج خاصة بالتسليح

يمكن الاستفادة منها بتوجيه ضربة ضد الأهداف المعادية. ومن أهم التعاريف في هذا المجال:

أ. المجال العسكري: معارك تستهدف السيطرة والاستيلاء على المقدرات المعلوماتية الإلكترونية للعدو والتحكم في شبكاته بعد اكتشافها والدخول عليها وإفسادها، مع توفير الحماية لمعلومات قواتنا مع إدراك تأثير التكنولوجيا الحديثة للمعلومات على ميدان المعركة.

ب. حرب المعلومات الشخصية: تعني الهجوم على خصوصية الأفراد بالتنصت عليهم ومراقبة شؤونهم الإلكترونية عبر البريد الإلكتروني، والعبث بالسجلات الرقمية وتغيير مُدخَلاتها المُخزَّنة في قواعد البيانات الخاصة بهم.

جـ. حرب المعلومات بين الشركات والمؤسسات: حرب تدور ضمن إطار المنافسة أكثر من العداء، وتعني قيام الشركات باختراق النظام المعلوماتي لمنافسها لمعرفة نتائج وتفاصيل أبحاثه العلمية الخاصة بالشركة أو المؤسسة، وقد تدمر البيانات الخاصة بمنافسها أو تستبدلها ببيانات زائفة.

وقد أصبح هذا المفهوم مع ثورة المعلومات يشير إلى استخدام المعلومات أو الهجوم على المعلومات كشكل من أشكال الحرب، ويمكن تعريفه بأنه أي فعل أو نشاط يستهدف حرمان العدو من معلوماته

أو استغلالها أو إفسادها أو تدميرها هي ووظائفها، وفي الوقت نفسه حماية النفس من هذه الأنشطة والأفعال (غيطاس، 2007: 6).

أما عن خصائص حرب المعلومات فيمكن تلخيص أبرزها في النقاط التالية:

1. ليس لها مسرح محدد للعمليات، فمسرحها أينما توجد المعلومة.
2. ليس لها توقيت، فالعدو هو الذي يحدد توقيت العمليات، وقد تبدأ دون أن يعلم الخصم بها.
3. الأسلحة المستخدمة من نوعية خاصة وجديدة وغير تقليدية وتتطلب متخصصين ذوي تأهيل علمي وتقني عالٍ.
4. زيادة العبء على أجهزة الاستخبارات ومراكز الدراسات لوضع كافة الاحتمالات والتوقعات وأساليب المواجهة موضع التنفيذ.
5. صعوبة تحديد ما يجب حمايته وأولويات الحماية ونقاط الضعف في المنظومة المعلوماتية.
6. صعوبة اكتشافها، وفي حال اكتشافها تكون قد بدأت العمل والتأثير فعلًا.
7. الدور المتنامي لإدارة الإدراك، فتقنيات المعلومات الجديدة ربما تزيد بشكل ملحوظ نشاطات التأثير وقوة الخداع، كما تؤدي إلى تعقيد جهود الحكومة في بناء دعم سياسي للمشاريع الأمنية ذات العلاقة.

إنّ القيام بحرب المعلومات سواء كان ذلك بقصد الدفاع أم الهجوم يتطلب التخطيط، وأن يعرف الطرف نفسه ويعرف خصمه، فمن الضروري أن يعرف نفسه للدفاع المثالي عنها، وأن يعرف خصمه للهجوم المثالي عليه، بالإضافة إلى ضرورة تحديد الأهداف. وفيما يلي ملخص للخطوات اللازمة لحرب المعلومات (البداينة، 2002: 182_183):

1. تحليل النظام (System Analysis): وهو تحديد العناصر والعقد الخاصة بالنظام والارتباطات بينها، وتقييم وظائف النظام مكان التحليل، ومطابقة النظم المادية مع المجالات المتنوعة للوظائف. وتوفر النتائج الناجمة عن هذا التكامل البيئة العملياتية الثابتة للنظام، وتؤدي إلى فهم النظام عامة.
2. تقييم الأهداف (Evaluate Objectives): وتتمركز الأهداف حول تحديد العُقَد الحساسة والارتباطات في نظم العدو، بحيث يمكن تحقيقها.
3. اختيار الأدوات (Select Tools): وفي حرب الفضاء الإلكتروني يمكن تحديد هذه الأدوات بالفيروسات، أو التشويش والإعاقة والتخريب، أو العمليات النفسية الإلكترونية.
4. تقييم الآثار (Assess Effects): وفي هذه الخطوة تتم مقارنة الآثار الفعلية مع الآثار المرغوب إحداثها في النظام الهدف (النظام المراد حمايته أو تدميره).

ولا شكّ في أنّ الفضاء الإلكتروني قد أصبح يعبر عن الساحة الخامسة للحروب المعاصرة، وأصبح من أهم أولويات الدول الأمنية تحقيق الأمن الإلكتروني الذي يضمن أمن وسلامة كافة منشآتها الإلكترونية، عبر تأسيس برامج متطورة لمواجهة التهديدات، وتحصين شبكاتها الإلكترونية، وتطوير وتطبيق تقنيات يمكن بواسطتها إلحاق الأذى بالأعداء. وبات على كلّ الدول أن يكون لديها قوة بشرية تتمثل بالخبراء الإلكترونيين القادرين على حماية بلادهم من أضرار الحروب والاختراقات الإلكترونية في جانبي الدفاع والهجوم.

وتتعدد الأشكال التي تظهر بها حرب المعلومات، لكن أبرزها:

1. حرب القيادة والسيطرة: هي الشكل الرئيسي لحرب المعلومات في ميدان القتال والصراع المسلح المباشر، وتكاد تقتصر على المجال العسكري، حيث تهدف إلى شلّ أنظمة القيادة والسيطرة للعدو على قواته ووسائل نيرانه، وكذلك أنظمة التوجيه والإنذار والمراقبة والاستطلاع.
2. حرب الاستخبارات: هي الشكل التقليدي لحرب المعلومات، فمع تقدم وسائل الاتصال والتكنولوجيا الحديثة تقلص وقت الحصول على المعلومات حتى كاد ينعدم، فأصبح هذا العمل مستمرًا، وهو يتطلب سرعة اتخاذ القرار وتنفيذه في الحال. وبصفة عامة تعد حرب الاستخبارات المدى الأوسع والأكثر استمرارية لحرب المعلومات.

3. الحرب النفسية: تهتم بالجانب الإنساني أو البشري لحرب المعلومات، وهي تهدف لمهاجمة عقل الخصم بشكل مباشر ليصل إلى حالة من اليأس والاستسلام والاقتناع بعدم جدوى المواجهة. ومن أهم أساليبها إطلاق الشائعات التي يُقدَر تأثيرها على الرأي العام للخصم بعد تحليل اتجاهاته.
4. حرب اختراق أنظمة الحواسب (القرصنة المعلوماتية): وهي تهدف إلى اختراق أنظمة الحواسب وشبكاتها بطرق غير شرعية لسرقة وتجارة المعلومات والبرامج.
5. حرب المعلومات الاقتصادية: وهي استخدام المعلومات للتأثير على اقتصاديات الدول أو المؤسسات المعادية.
6. حرب الفضاء أو حرب الشبكات (Net Cyber Warfare): هي النمط المستقبلي لحرب المعلومات، حيث يتم العمل للسيطرة على البيئة الشاملة المعلوماتية بين النظم والشبكات عبر الفضاء.

• القرصنة الإلكترونية

يشير مفهوم القرصنة الإلكترونية إلى استخدام وسائل الاتصال وتكنولوجيا المعلومات الحديثة في ممارسات غير مشروعة، تستهدف التحايل على أنظمة المعالجة الآلية للبيانات، لكشف البيانات الحساسة (المُصنَّفة) أو تغييرها والتأثير على سلامتها أو حتى إتلافها. وبعبارة أخرى: ليست القرصنة سوى عملية دخول غير مُصرَّح به إلى أجهزة

الآخرين وشبكاتهم الإلكترونية، أي أن توجه هجمات إلى معلومات الكمبيوتر وخدماته، بقصد المساس بالسرية أو المساس بسلامة المحتوى عليه، أو تعطيل كفاءة الأنظمة وقدرتها على القيام بأعمالها. فهدف هذا النمط الإجرامي هو نظام الكمبيوتر، وبشكل خاص المعلومات المخزنة داخله. فالقرصنة – إذًا – تعني الوصول بطريقة غير مشروعة من خلال ثغرات نظام الحماية الخاص بالهدف (محمود، 2005: 147).

ويمكن تقسيم القائمين بأعمال القرصنة الإلكترونية كالتالي:

1. الْهُواة (الهاكرز): (Hackers)

يعتمد الهواة على برامج التجسُّس الجاهزة والمتاحة في كل مكان، سواء عن طريق الشراء أم التحميل من شبكة الإنترنت، ويقوم الهاكرز بزرع ملفات التجسس (patches &Trojans) في حواسيب الضَّحايا عن طريق البريد الإلكتروني أو ثغرات الويندوز التي يكتشفها البرنامج. هذا الصِّنف من الهاكرز أهدافه طفوليَّة، حيث يسعى لإثبات نجاحه في استخدام هذه البرامج، وانضمامه إلى قائمة الهاكرز بهدف التفاخر بين الأصحاب كشخص يمتلك مواهب يفتقدها بعضهم. وهؤلاء الهواة كلُّ ما يشغلهم هو التسلل إلى حواسيب الآخرين وسرقة بريدهم الإلكتروني، والتلاعب في إعدادات هذه الأجهزة، مع تَرْك ما يفيد أنهم فعلوا ذلك كشكل من أشكال الغرور والتباهي بالنفس (شواريتو، 2008: 139).

2. المحترفون (الكراكرز) :Crackers

أما المُحترفون فهم الفريق الأخطر، لأنهم يعلمون ماذا يريدون، وماذا يفعلون، ويتقنون كيفية الوصول إلى أهدافهم باستخدام ما لديهم من علم يطوِّرونه باستمرار، بالإضافة إلى استخدام البرامج الجاهزة المتطورة. وهم يعتمدون على خبرتهم في لغات البرمجة والتشغيل، وتصميم وتحليل وتشغيل البرامج بسرعة، كما أنّ هواياتهم الأساسية هي معرفة كيفيَّة عمل البرامج لا تشغيلها. إنَّ أهداف هذا الفريق أكبر وأخطر من الفريق السابق، فأهدافهم هي المصارف وسحب الأموال من حساب العملاء، أو الولوج إلى أخطر المواقع وأكثرها حساسية، والتلاعب ببياناتها أو تدميرها (الجهيني، 2006: 28).

وهناك – في الحقيقة – العديد من الأدوات والوسائل الشائعة في إجراء عمليات القرصنة الإلكترونية وهي:

1. **البرامج الخبيثة:** ويُستخدَم لفظ (Malware) أي البرامج الخبيثة للإشارة إلى مجموعة واسعة من البرمجيات كالفيروسات والديدان وحيل تصيد المعلومات. وتحاول هذه البرامج استغلال العيوب الموجودة في البرامج الأخرى والأخطاء التي يقع فيها مستخدمو الحاسوب قبل الدخول إلى المواقع المصابة بالعدوى الفيروسية أو فتح مُرفَقات الرسائل البريدية. والفيروسات هي برامج يتم تمريرها من مستخدم إلى آخر عبر الإنترنت أو الوسائط المحمولة مثل وحدات التخزين الصغيرة Flash drivers، أما

الديدان فلا تتطلب تمرير برنامج إلى مستخدم آخر لأنها قادرة على نسخ نفسها ذاتيًا باستغلال عيوب معروفة ثم تزحف كالديدان عبر الإنترنت.

2. **حيل اصطياد المعلومات** (Phishing Scams): تقوم على خداع مستخدِم الإنترنت للإدلاء بمعلومات مثل أرقام الحسابات المصرفية وشيفرات المرور، وذلك عن طريق إنشاء رسائل بريد إلكتروني ومواقع زائفة توهم المستخدِم بأنها متعلقة بعمليات تجارية حقيقية كما في حالة المصرف الذي يتعامل معه (ليبيك، 2007: 47).
3. **ثغرة تسلل:** (Trapdoors): هي برنامج حاسوب غير مُرخَّص يضاف إلى برنامج ما لأغراض خبيثة، ويسمح بالولوج غير المُرخَّص به إلى شبكة أو برنامج حاسوبي. فغالبًا بعد أن يقوم القراصنة باختراق النظام أو الشبكة لأول مرة، يتركون وراءهم ثغرة تسلل للسماح لهم بالدخول في المستقبل بطريقة أسرع وأسهل. ويشار إليه أيضًا باسم (Trojan) نسبة إلى حصان طروادة، وهو استلهام للخدعة التي قام بها محاربو الإغريق لاقتحام طروادة عندما تظاهروا بالانسحاب تاركين وراءهم تمثالًا لحصان خشبي، وقد اختبأت داخله قوة من المحاربين الأشداء، وتسللوا إلى طروادة واحتلوا المدينة (بنور، 2015: 88).

وأحيانا تسمح ثغرات التسلل للقراصنة بالدخول إلى أجزاء معينة من الشبكة لا يُسمَح لهم بالدخول إليها عادة، وعندما يخترقون

برنامجًا ما لا يزال قيد التطوير، فإنّهم لا يسرقون نسخة منه فحسب، بل قد يضيفون إليه شيئًا ما، وقد تسمح لهم ثغرات التسلل أحيانًا بالوصول إلى الجذر (Root)، ومعنى ذلك أنّ لديهم السلطات والصلاحيات التي يتمتع بها مصمم البرنامج أو مدير الشبكة، وأنهم يستطيعون إضافة ما يشاؤون من برمجيات ويمحون أي دليل على وجودهم (جواد، 2016: 134).

4. **القنبلة المنطقية (logic Bomb)**: وهي تطبيق من تطبيقات الحاسوب أو سلسلة من التعليمات تسبب توقف النظام أو الشبكة عن العمل و/ أو حذف كل البيانات الموجودة على الشبكة، ويُنسَب اختراع القنابل المنطقية إلى الجيش الأمريكي. وهناك أدوات أكثر تقدمًا من القنابل المنطقية يمكنها أن تبدأ بتوجيه أوامر لمعدات الحاسوب لتقوم بشيء معين يؤدي إلى تدمير، كأن تأمر شبكة الكهرباء بتوليد حمل كهربائي زائد يؤدي إلى حرق الدوائر الموجودة في محولاتها، أو تجعل لوحات التحكم في الطيران تدفع الطائرة إلى السقوط المفاجئ، وبعد ذلك تمحو كلّ شيء ثم تمحو نفسها أيضًا.

5. **إرسال طوفان من طلبات الاتصال** إلكترونيًا بالأجهزة الخادمة التي تدعم معظم صفحات الإنترنت المستخدمة، وإغراق الأجهزة بهذه الطلبات بحيث تتعطل نتيجة عدم احتمال الحمل الشديد، وعجز عدد آخر من الأجهزة الخادمة نتيجة لتكدس نبضات،

واستدعاء صفحات لا يمكن الولوج إليها أساسًا، وهذا ما يسبب عجزًا عن إجراء أي معاملات مصرفية أو الدخول إلى مواقع الصحف أو الانتفاع بالخدمات التي توفرها الحكومة. وقد يقوم مستخدِم الحاسوب بفتح صفحة على الإنترنت تؤدي إلى تنزيل برنامج يحوّل هذا الحاسوب إلى جهاز مستلَب وخاضع للتحكم عن بعد. ويمكن للمرء أن يفتح رسالة بريد إلكتروني، فيبدأ معها تنزيل البرنامج الذي يتحكم في الحاسوب، وفي بعض الأحيان يبقى الحاسوب المستلَب كامنًا في انتظار الأوامر، بينما يقوم في أحيان أخرى بالبحث عن أجهزة أخرى لمهاجمتها، وعندما ينشر عدواه إلى أجهزة أخرى تقوم هذه الأجهزة بنقل العدوى إلى غيرها من الأجهزة، لتنشأ الظاهرة المعروفة باسم (العدوى الدودية)، بمعنى أنّ العدوان يستشري ويتغلغل كالديدان من جهاز واحد إلى آلاف أو ملايين الأجهزة، وكلّ ذلك يمكن حصوله في بضع ساعات فقط (محمود، 2005، 12).

6. **إنشاء شبكات تجريبية مسلوبة الإدارة (Botnet):** وهي أجهزة الحاسوب التي تُجبَر على العمل وفقًا لأوامر مستخدم بعيد غير مُرخَّص له باستخدامها، وعادة ما يتم ذلك من دون علم أصحاب الشبكة أو مديرها، وتُستغَل هذه الشبكة المكونة من أجهزة الحاسوب الروبوتية في الهجوم على أنظمة أخرى، وعادة ما يتحكم في الشبكة المُسيَّرة حاسوب واحد أو أكثر، وكثيرًا ما يشار إلى أجهزة

الحاسوب المتصلة بالشبكة المُسيَّرة بكلمة (Zombies) أي مسلوبة الإدارة، وتستخدم الشبكات المُسيَّرة لأغراض عديدة، مثل إغراق الشبكات بالرسائل (بدران، 2010: 14).

7. **آلية تخطي الحاجز (over flow Buffer)**: وهي عبارة عن كتابة خطأ في شيفرة الحاسوب يسمح لمستخدم غير مرخص له بالدخول إلى شبكة معينة. ويتمثل هذا الخطأ في عدم وضع حد لعدد الحروف والرموز التي يمكن إدخالها من جانب مستخدم غير موثوق به، فيتمكن هذا الأخير من إدخال تعليمات إلى نظام البرنامج (جواد، 2016: 136).

8. **قطع خدمة الإنترنت** عن طريق الإغراق الموزَّع (DDoS) (Distributed Denial of Services): وهو أسلوب من الأساليب الأساسية لحرب الفضاء الإلكتروني، يستخدم لإغراق مواقع معينة على الإنترنت أو جهاز خادم أو راوتر (Router) بطلبات للبيانات تفوق طاقة الموقع على الردّ أو المعالجة، ونتيجة لهذا الطوفان تعجز التحركات المشروعة عن الوصول إلى الموقع، فيصبح في حكم المغلَق. وتُستخدَم الشبكات المُسيَّرة لتنفيذ هذه الهجمات، ومن ثم زرعها على آلاف الأجهزة المصدرة للرسالة، والتي تعمل معًا في آن واحد. وهناك آلية أخرى وهي آلية التشفير (Encryption) وهي خلط المعلومات بطريقة لا يمكن قراءتها لمن ليس لديه مفتاح فك الشيفرة، ويؤدي تشفير

التحركات (البيانات الكامنة) إلى منع كلّ من يعترضها أو يحاول سرقتها من قراءتها (كلارك، 2012: 237).

تسعى العديد من دول العالم إلى وضع القوانين والتشريعات الجنائية لمواجهة الجرائم الإلكترونية، وإجراء تعديلات في القواعد الإجرائية، بتطوير أساليب كشف وضبط هذه الجرائم بما يحقق متطلبات الحماية الإلكترونية من أساليب القرصنة في مجال تقنية المعلومات والاتصالات، فمِن خلال استعراض أدوات وأساليب القرصنة السابق ذكرها، يمكن تلخيص التأثيرات الضارة للقرصنة على أمن المعلومات الإلكترونية فيما يلي:

1. تهديد قطاعات البنى التحتية: ويمكن تصنيفها إلى خمسة قطاعات حسب الخصائص المشتركة بينها (البداينة، 2002ـ 36):

أ. قطاع الاتصالات والمعلومات: ويشمل شبكة الاتصالات العامة، والإنترنت، والحاسبات في المنازل، والاستخدام الأكاديمي، والحكومي، والتجاري.

ب. قطاع التوزيع الفيزيقي: ويشمل الطرق السريعة للمواصلات، وخطوط السكك الحديدية، والموانئ، وخطوط المياه، والمطارات، وشركات النقل، وخدمات الشحن التي تسهل انتقال الأفراد والبضائع.

ج. قطاع الطاقة: ويشمل الصناعات التي تنتِج الطاقة، وتوزع الطاقة الكهربائية، والبترول والغاز الطبيعي، ومنشآت تخصيب اليورانيوم والمفاعل النووي.

د. قطاع المال والبنوك: ويشمل البنوك وشركات الخدمات المالية من غير البنوك، ونظم الرواتب، وشركات الاستثمار، والقروض المتبادلة، والتبادلات الأمنية والمادية.

2. تهديد الأمن المعلوماتي للحكومة الإلكترونية: وتشمل تشويه المواقع الإلكترونية أو تدميرها، والعبث بالبيانات من خلال تغييرها أو إنشاء بيانات وهمية، بالإضافة إلى الأخطار المادية المتمثلة باستدعاء الخبراء الفنيين لسدّ الثغرات التي يدخل منها القراصنة.

3. تهديد القطاعات العسكرية من خلال الدخول إلى بيانات برامج تصنيع الأسلحة والقيام بسرقتها أو تدميرها أو تزييفها، بالإضافة إلى التهديدات الإلكترونية للقراصنة أثناء العمليات العسكرية في الحروب، إذ تقوم قيادة الحرب اليوم على مجموعة اتصالية رقمية تتكون من شبكات كثيفة للرصد والإعلام والاتصال والتحديد الجغرافي والتنصت الإلكتروني والتشويش وفكّ الرموز والتحليل والمحاكاة، وتعتمد المواجهات على عمليات موجهة عن بعد تنجزها روبوتات Robots من كلّ الأنواع على الأرض والبحر وفي أعماق البحار وفي الجو وفي الفضاء. ويقتضي هذا العالم الرقمي إعادة بناء

الدفاع والاستراتيجيات على نحو مُعمَّق، ولا سيّما أنّ الاعتداءات يمكنها أن تصدر من أي مكان وفي أي لحظة (بنور، 2015: 93).

• استخبارات المصادر المفتوحة

أحدث الفضاء الإلكتروني ثورة في عمل أجهزة الاستخبارات الدولية، ودخلت هذه الأجهزة في تحديد أهداف ومهام ومراحل تنفيذ الأنشطة الاستخباراتية التي تتم في المجال الخارجي وداخل الدول، واستفادت تلك الأجهزة من توافر كم هائل من المعلومات، بعد أن كانت تعاني في السابق شحًا في مصادر المعلومات، وصعوبات في التحليل. وكان لتكنولوجيا المعلومات والاتصال دور في معالجة البيانات في أسرع وقت، وبأقل جهد وبأقل تكلفة، والخروج من ذلك بتحليلات كمية تساعد في بناء التوقعات المستقبلية، والمساعدة في النهاية على طرح البدائل والخيارات المناسبة التي تسهم في عملية صنع القرار.

فالثورة التي تعايشها مصادر المعلومات أسفرت عن تطور هائل في نوعية هذه المصادر وتماشى ذلك مع تطور وحجم المعلومات والنوعية التي تحتويها، فبقدر تعاظم حجم وتنوع المعلومات تعاظَم بالدرجة نفسها حجم مصادر المعلومات وتنوعها بصفة عامة.

وقد عُرِّفت المصادر المفتوحة بأنها مواقع تحتوي على معلومات ذات طبيعة عامة ومفتوحة، وتضم كافة الوسائل المتاحة للحصول على المعلومات غير المحظورة، ومن أهمها الصحف والتلفاز والإذاعات

والكتب والتقارير والصور ومواقع الإنترنت والخرائط والمعارض والندوات ومراكز الأبحاث وغيرها (السبيعي، 2013: 74). وتتبلور مميزات المصادر المفتوحة بما يلي:

1. أنّ المعرفة المستقاة منها ذات قيمة شمولية، بمعنى أنها تغطي مجالات الاهتمامات الإنسانية كافة، سياسيًا واجتماعيًا واقتصاديًا وعسكريًا وعلميًا وتكنولوجيًا، بما يحقق فوائد جمة، ويعطي هذه المصادر قوة جذب هائلة للمتعاملين معها من مختلف الفئات الحكومية والخاصة لتغطية احتياجاتهم في وضع السياسات واتخاذ القرارات (الشعلان، 2000: 193).
2. أنّ التعامل مع هذه المصادر يتسم بسهولته ومشروعيته، حيث لا توجد قيود نظامية تحول دون الاستعمال المشروع لهذه المصادر والتي تتسم بصفة العمومية، أي الإتاحة لجميع الناس (NATO، 2001: 2)
3. المصادر المفتوحة تتصف بميزة التحديث المستمر للمعلومات الذي لا يتوقف للحظة واحدة، مما يزيد من فاعلية الاستفادة من المعارف التي تقدمها في شتى المجالات (قنديلجي، 2000: 110). وهي مصدر مستمر التدفق للمعلومات، واحتمال توقفها نادر الحدوث غالبًا (كامل، 1995: 73).
4. كفالة السرعة في الحصول على أي قدر من المعلومات مهما تزايد حجمها، وهي الميزة التي تتحقق بصفة خاصة في مصادر المعلومات

المفتوحة حديثة النشأة التي ابتُكِرت باستخدام سرعة الحركات الإلكترونية، والتي مكنت من تزايد مُطَّرِد في سرعة تجميع البيانات وإظهارها وعرضها بشتى أنواعها، بما يهيئ الفرصة لسرعة الاستفادة منها، وبصفة خاصة في مجال وضوح الرؤية أمام متخذ القرار، فيصدره في أسرع وقت وبأكبر قدر من الرشد (أبو زيد، 1985: 94).

5. أنّ استمرارية المصدر المفتوح في بث المعلومات، ومتابعة حاضر هذه المعلومات وما يتصل بالمستقبل من توقعات، يُمَكّن أجهزة الأمن من الحصول على احتمالات مستقبل تطور المعلومات، ويعطيها القدرة على التنبؤ بمسارها المستقبلي، وهو من أهم عناصر المعلومة الأمنية التي توفر إمكانية الاستعداد لمخاطر أمنية متوقَّعة الحدوث (الشمسي، 1999: 67).

6. سهولة تناقل معلومات المصادر المفتوحة بين الأجهزة الأمنية بسرعة تغطي كافة المستويات الأمنية المطلوب إحاطتها علمًا بهذه المعلومات، وذلك من خلال تعدد الوسائط التي تنتقل معلومات هذه المصادر من خلالها.

ومصطلح استخبارات المصادر المفتوحة (Open Source Intelligence) يعني عمليات الاستخبارات التي تستخدم المصادر المفتوحة من المصادر غير المحظورة. وكغيرها من بقية الأنواع من الاستخبارات لا تتوقف استخبارات المصادر المفتوحة عند جمع المعلومات، بل تشمل تحليل

المتطلبات وتصفية المعلومات وتحليلها، وتكاملها بعد جمعها. ويهدف هذا النوع من المعلومات إلى المساعدة في الحصول على إجابات مهمة لهدف ما، وقد يتم جمع معلومات حساسة من مصادر متعددة غير محظورة، ويتم دمجها لتشكل وحدة متكاملة، أو قد يتم استنساخ معلومات هامة من المعلومات المُجمَّعة من المصادر العامة (البداينة، 2002: 218).

ويمكن توضيح العلاقة بين المعلومات وعملية اتخاذ القرار على صورة المعادلة التالية:

الملاحظة + التمعن والتفكير فيها ← البيانات

البيانات + التجميع + التحليل + التنظيم ← معلومات

المعلومات + التجميع + التنظيم + الاستيعاب ← معرفة

المعرفة + العقل ← حلّ + قرار + تقدم.

وتُعتَبر مصادر المعلومات الإلكترونية من أبرز مصادر المعلومات المتداولة عالميًا، وتغطي المعارف التي تتضمنها التخصصات العلمية الدقيقة المختلفة، إلى جوار المعلومات الإخبارية العامة، والمعلومات التجارية وغير التجارية. وتتاح جميع هذه المعلومات إمّا بصورة نصية كاملة، أو تُقدَّم في مختصرات وافية. وقد أصبحت مصادر المعلومات الإلكترونية بهذا الشكل قسمًا مستقلًا بذاته، يقف جنبًا إلى جنب مع

مختلـف مصـادر المعلومـات التقليديـة كالصـحف الورقيـة، والإذاعـة، والتلفاز، ومراكز المعلومات... وغيرها.

وكـان لتطبيقـات تكنولوجيـا المعلومـات والاتصـال دور في معالجـة البيانـات بأسـرع وقـت، وبأقـل جهـد، وبأقـل تكلفـة، والخـروج مـن ذلـك بتحليـلات كميـة سـهلة تسـاعد في عمليـات التحليـل، وفي بنـاء التوقعـات والتنبؤات المستقبلية، والمساعدة في النهاية على طرح البدائل والخيارات المناسبة التـي تسـهم في عمليـة صـنع القـرار (عبـد الصـادق، 2014: 166)، فقد أصبح استخدام الحاسبات الإلكترونية لتجميع المعلومات وتحليلهـا وتخزينها واستعادتها عنـد حاجتهـا ضـرورة لا غنـى عنهـا لجميـع الـدول. وهناك العديد مـن الأدوات والوسـائل الإلكترونيـة المسـتخدمة في مجـال استخبارات المصادر المفتوحـة الإلكترونيـة، ويمكـن تلخـيص أهـم هـذه الأدوات كما يلي (البداينة، 2002: 218_219):

1. المتصفحات (Browsers): وهي برامج التصفح على الإنترنت، ومـن أشهرها نتسكيب (Netscape) وإكسبلورر (Explorer).
2. بروتوكـول الـنص الفـائق (HTTP): حيـث يُمَكِّـن بروتوكـول الـنص الفائق مواقع الإنترنت والمتصفح من الاتصال وتبادل الوثائق والصور والصـوت. والمصـطلح الفنـي لموقـع صـفحة مـا هـو مـا يعـرف (Uniform Resource Locator, URL)، وهو ما يمكن تتبعه لمعرفـة المعلومات التي يرسلها متصفحك إلى كل صفحة طلبتها.

3. محركـات البحـث (Search Engines): وهـي أدوات علـى شـبكة الإنترنـت تُمَكِّـن مـن البحـث عـن المعلومـات، وهـي كثيـرة أهمهـا (Yahoo, Google, Hotbot, AltaVista)، ويـوفر بعضـها خاصـية البحث عـن الأفـراد، ومـن الممكـن أن تبحـث تحـت مواقـع الـبرامج المجانية وتكشف معلومات عنك.

وهنـاك العديـد أيضًـا مـن الـبرامج والمواقـع الإلكترونيـة التـي يمكـن استخدامها كمصـدر مهـم للمعلومـات، ومـن أبـرز هـذه المصـادر مواقـع التواصـل الاجتمـاعي. ويمكـن القـول أنـه نتيجـة لتقـارب التكنولوجيـات وقعـت ثلاثـة أشـياء: أولًا، كانـت كتلـة حرجـة مـن الهواتـف الذكيـة مـع اتصالات الجيل الثالث في أيدي مـواطنين عـاديين، ثانيًـا، يسـتخدم هـؤلاء المواطنون عددًا قليلًا من التطبيقات لتقاسـم كميـة ضـخمة مـن المحتـوى حول الأحداث السياسية داخـل بلـدانهم، ثالثًـا، كانـت هـذه البيانـات حـرة ومجانية لبقية العالم من حيث الوصول إليهـا وتحليلهـا (Gabriel، 2006: 55).

ومـن المنـاهج المُسـتخدَمة في اسـتخبارات المصـادر المفتوحـة مـنهج جنــوة (Genoa)، وهــو خلــيط مــن تقنيــة المعلومــات والبرمجيــات التعاونية (collaborative software)، ويُعنَـى بتجميـع الأطـراف المعنيـة ليزيد من عمق التحليل وسـرعته، ويقـوم علـى ثلاثـة مبـادئ رئيسـية، هـي: الشفافية، وتواصـل المعلومـات، وبيئـة متماسـكة، فـإذا تـوافرت الشـفافية

يمكن أن يخضع كل ما ينتجه محللو الاستخبارات لدراسة صناع القرار الذين يمكنهم أخذ المنتَج وإعادة إنتاجه، أو الولوج في العملية التي جاءت بالمنتَج. ويتصف التواصل بالأهمية أيضًا، فنحن نحتاج إلى ذاكرة موحّدَة ليس لحفظ المعلومات فقط، ولكن لكي نكون قادرين على التعامل البارع معها لاحقًا، أي أن نكون قادرين على إثارة تساؤلات على أساس قواعد البيانات للتجربة السابقة. لقد صممت البيئة المتماسكة لمنهج (جنوة) لتضمن أنّ كلّ الأدوات تعمل معًا لكي توفر الشفافية والتواصل.

ويستخدم منهج (جنوة) بيئة قوية مبنية على الموقع في الشبكة العالمية تُسهّل التفكير المبدع. وتتلخص الفكرة في تحاشي استخدام تسلسل الأفكار القياسي، ويهدف المنهج إلى توسيع نطاق احتمالات التفكير التخيلي، وإلى دراسة عدد أكبر من الحجج المختلفة، والوصول إلى بدائل أكثر دقة ووضوحًا، ونكتسب كل ذلك من التقنية التي يتم الآن تطويرها بمنهج جنوة. ويتبع هذا المنهج مقاربة ثلاثية الشعب فيما يتعلق بالزمن، فنحن نستخدم ذاكرة موحّدَة في شكل قواعد بيانات لتطوير المسارات الحالية للأزمة، وهذه المسارات بدورها لها القدرة على تطوير تخطيط مبني على السيناريو المتعلق بالمستقبل. إنّ فكرة الذاكرة الموحّدَة قد تثير جدلًا لأنها تسمح للمرء بالعودة في وقت لاحق لتحديد من قام بأكثر التحليلات نجاحًا.

وفي ضوء التقديم السابق يمكننا أن نضع استخبارات المصادر المفتوحة ضمن نموذج واقعي يتمثل في التأكد من صحة المعلومات المستقاة من المصادر المفتوحة، ومقاطعة المعلومات في جميع المصادر المفتوحة المستخدَمة، ومن ثم التأكد من الفهم الصحيح للمعلومة من خلال التحليل المتصل، بعد التعرف على محتويات المصدر المفتوح كاملة، وما تحتويه من ملفات وصفحات، كالوسائط التي يستخدمها المصدر المفتوح لإيصال المعلومات ونشرها، ومن ثم الإدارة العلمية لتقديم التقارير الداعمة لعملية صنع القرار.

• الجانب المظلم لاستخبارات المصادر المفتوحة

من المهم جدًا في هذه المرحلة معالجة المشكلة الرئيسية المتعلقة باستخبارات المصادر المفتوحة، وهي: إذا كان هناك شيء متاح بسهولة لمحللي أجهزة الدولة، فإنّه متاح أيضًا للجهات الفاعلة المهدِّدة.

تستخدم الجهات الفاعلة في مجال التهديد أدوات وتقنيات استخبارية مفتوحة المصدر لتحديد الأهداف المحتملة، واستغلال نقاط الضعف في الشبكات المستهدفة بمجرد تحديد نقطة الضعف، وغالبًا ما تكون عملية سريعة وبسيطة للغاية لاستغلالها وتحقيق مجموعة متنوعة من الأهداف الخبيثة.

وهذه العملية هي السبب الرئيسي وراء اختراق العديد من الشركات الصغيرة والمتوسطة كل عام، ليس لأنّ مجموعات التهديد تهتم بها على وجه التحديد، بل بسبب الثغرات الموجودة في شبكتها أو بنية موقعها على الويب، إذ يتم بناء هذا الموقع باستخدام تقنيات استخبارات بسيطة مفتوحة المصدر تجعل منها أهدافًا سهلة.

ولا تعمل استخبارات المصادر المفتوحة على تمكين الهجمات التقنية على أنظمة وشبكات تكنولوجيا المعلومات فقط، بل يسعى ممثلو التهديد أيضًا إلى الحصول على معلومات حول الأفراد والمنظمات التي يمكن استخدامها لإمداد حملات الهندسة الاجتماعية المتطورة باستخدام التصيد الاحتيالي (البريد الإلكتروني)، والتزييف (الهاتف أو البريد الصوتي)، و(SMS) في كثير من الأحيان، ويمكن استخدام المعلومات التي تبدو غير ضارة، والتي يتم مشاركتها من خلال الشبكات الاجتماعية والمدونات لتطوير حملات هندسة اجتماعية مقنعة للغاية، ولكنّها تُستخدَم بدورها لخداع المستخدِمين ذوي النوايا الحسنة لتهديد شبكة مؤسستهم أو أصولها.

وهذا هو السبب في أنّ استخدام استخبارات المصادر المفتوحة لأغراض أمنية مهم جدًا، فهو يمنح الفرصة للعثور على نقاط الضعف في شبكات الدولة وإصلاحها، وإزالة المعلومات الحساسة قبل أن يستخدم الفاعل المُهدِّد نفس الأدوات والتقنيات لاستغلالها.

• الدبلوماسية الرقمية

تشير الدبلوماسية في العصر الرقمي إلى الأدوات والأساليب الجديدة لإجراء الدبلوماسية بمساعدة الإنترنت وتكنولوجيا المعلومات والاتصالات، ويمتد تأثيرها إلى الممارسات الدبلوماسية المعاصرة، حيث تؤثر التكنولوجيا في الدبلوماسية والطريقة التي تُمارَس بها بعدد من السبل، وتمتد كذلك إلى تحديد الجهات الفاعلة الجديدة وأدوات وعمليات الدبلوماسية والعلاقات الدولية، وتشمل المصطلحات ذات الصلة: الدبلوماسية السيبرانية التي تتعلق بشكل رئيسي بالقضايا الأمنية، ثم دبلوماسية التكنولوجيا والعلوم المتعلقة بأنماط تفاعلات الدول في محاور الابتكار، ودبلوماسية البيانات المتعلقة باستخدام وتأثير البيانات الضخمة على الدبلوماسية والشؤون الدولية، والتجارة الإلكترونية المتعلقة بالقضايا الاقتصادية.

وتُعبِّر الدبلوماسية في بلد ما عن عدة أنشطة، منها تمثيل مصالح هذا البلد ورعاياتها، وتوفير المعلومات للسلطات، والتفاوض، والتفاعل مع المجتمع المدني، ولا سيّما قادة الرأي في بلد الإقامة، وحماية رعايا البلد. وتعتبر الدبلوماسية الرقمية امتدادًا للدبلوماسية بمفهومها التقليدي، وهي تستند إلى الابتكارات وأنواع الاستعمال الناجمة عن تكنولوجيات المعلومات والاتصالات، بَيدَ أنّ الأدوات الرقمية التي تمثل وسيلة لنقل المعلومات تساهم في تغيير وجه النشاط الدبلوماسي.

أثَّـر الإنترنـت وتكنولوجيـا المعلومـات والاتصـالات الجديـدة في الدبلوماسية على نطاق واسع، حيث أضحت التكنولوجيات الجديدة الآن أدوات لممارسة الدبلوماسية، وأصبحت جزءًا من جداول أعمال صانعي السياسات الدولية، والمتغيرات التي تؤثر في بيئة الدبلوماسية. وتظهر الدبلوماسية في العصر الرقمي من خلال التركيز على كيفية استخدام الدبلوماسيين للأدوات الإلكترونية (الدبلوماسية الرقمية)، وكيف تتم مناقشة تطوير التقنيات الجديدة وآثارها كجزء من جدول الأعمال الدبلوماسي (إدارة الإنترنت)، وكيف أعادت التقنيات الجديدة تعريف التعاون الدولي والاعتماد المتبادل (التعاون الرقمي).

تم وصف الدبلوماسية الرقمية لأول مرة في عام 2001، وعرّفها البعض بأنها الاستخدام المتزايد لتكنولوجيا المعلومات والاتصالات ومنصات وسائل الإعلام الاجتماعية في إدارة الدبلوماسية العامة. ويعتقد من يتبنون هذا التعريف أنّ الوسيلة هي التي تغيرت وليس الرسالة، حيث أصبح الدبلوماسي يتواصل مع الجماهير الأجنبية الآن من خلال قناة تويتر، بدلًا من التحدث إليهم عبر الراديو.

ويعتقد البعض الآخر أن الدبلوماسية الرقمية هي أكثر من مجرد أداة جديدة في صندوق الأدوات المستخدمة، إذ يمكن لأية سفارة الآن إقامة اتصالات ثنائية الاتجاه مع أتباعها من خلال قناتها على تويتر. ويمكن للدبلوماسيين الآن التحدث مع الجماهير الأجنبية من خلال الرد على

المنشورات على ملفاتهم الشخصية في (فيس بوك) مثلًا، بدلًا من التحدث إليهم من خلال التلفزيون. وهذا هو الحوار الذي أصبح ممكنًا بفضل الدبلوماسية الرقمية التي يمكن أن تحلّ محل نمط الدبلوماسية العامة، حيث يوفر مثل هذا الاتصال ثنائي الاتجاه المزيد من الفرص للمشاركة مع الجمهور الأجنبي، والمشاركة التي قد تسهل إنشاء العلاقات بين دولة وسكان دولة أخرى.

إنّ التفاعل بين الإنترنت والدبلوماسية يمكن تصوره في ثلاثة جوانب:

1. التغييرات التي يقودها الإنترنت في البيئة التي تجري فيها الدبلوماسية (الجغرافية السياسية، والاقتصاد الجغرافي، والسيادة، والتماسك الاجتماعي).
2. ظهور مواضيع جديدة حول جداول الأعمال الدبلوماسية (إدارة الإنترنت والأمن السيبراني والخصوصية).
3. استخدام أدوات الإنترنت الجديدة في ممارسة الدبلوماسية (وسائل التواصل الاجتماعي والبيانات الضخمة).

لقد أصبح Twitter و Facebook حاليًا أكثر الأدوات الإلكترونية شيوعًا التي تستخدمها وزارات الخارجية حول العالم، وتُعتبَر هاتان الشبكتان من الأمثلة الجيدة على الأنظمة الأساسية المتكاملة، لأنه يمكن ربطها بعضها ببعض، مما يدفع حركة المرور من منصة إلى أخرى.

يسمح تويتر للمستخدم بالتعبير عن آراء المجتمع حول قضايا مختلفة، والانخراط في مناقشات مع الآخرين لتقديم وشرح المواقف الخاصة، وتحديد المقالات والقراءات حول مواضيع معينة ذات أهمية من خلال المشاركات التي تم وضع علامة #hashtags عليها. ويتم استخدام فيس بوك بشكل متزايد للتواصل الاحترافي أيضًا، من خلال إنشاء ملفات شخصية أو صفحات شخصية أو مجموعات ذات اهتمامات محددة أو أحداث مؤسسية أو عامة، ويمكن للمؤسسة جمع مجتمع مهتم بعمله، وتنظيم المحتوى، والمشاركة بكفاءة مع المجتمع والجمهور. وتشمل الأنظمة الأساسية الأخرى مثل YouTube وLinkedIn و Pinterest و Instagram أدوات إلكترونية مهمة للدبلوماسية العامة، وباتت تُستخدَم بشكل مكثف من الدبلوماسيين لنشر الرسائل والتواصل.

• الجانب المظلم من الدبلوماسية الرقمية

تحمل المنصات الرقمية – مثل العديد من التقنيات الأخرى – تحديًا مزدوج الاستخدام، وهو أنه يمكن استخدامها من أجل السلام أو الحرب، للخير أو الشر ، للهجوم أو الدفاع.

ويمكن استخدام الأدوات نفسها التي تسمح لوزارات الخارجية والسفارات بالتواصل مع ملايين الأشخاص وبناء جسور «رقمية» مع

الجمهور عبر الإنترنت، بهدف تعزيز التعاون الدولي أو تحسين مشاركة المغتربين أو تحفيز العلاقات التجارية أو إدارة الأزمات الدولية، تُستخدَم هذه الأدوات أيضًا كشكل من أشكال «القوة» لاختراق البيئات السياسية والإعلامية في البلدان المستهدفة، وتقويض النسيج السياسي والاجتماعي لهذه البلدان.

وقد اتسع «الجانب المظلم» من الدبلوماسية الرقمية في السنوات الأخيرة، وقد أشير من خلاله إلى الاستخدام الاستراتيجي للتكنولوجيا الرقمية كأدوات لمواجهة التضليل والدعاية من قبل الحكومات والجهات الفاعلة من غير الدول سعيًا لتحقيق المصالح الاستراتيجية، إلى درجة بدء ظهور آثار خطيرة لها على النظام العالمي.

وعلى سبيل المثال ، تعرض أكثر من 150 مليون أمريكي لحملة تضليل روسية قبل الانتخابات الرئاسية لعام 2016، حيث أثبت تقرير أعده مجلس الشيوخ الأمريكي أنّ حملة التضليل التي قامت بها روسيا حول انتخابات 2016 استخدمت كل منصة رئيسية لوسائل التواصل الاجتماعي لتقديم الكلمات والصور ومقاطع الفيديو المصممة خصيصًا لمصالح الناخبين للمساعدة في انتخاب الرئيس ترامب، وزعم أنها عملت بجد أكثر لدعمه أثناء وجوده في منصبه. كما كانت حملات التضليل الروسية نشطة للغاية في أوروبا، من خلال السعي في المقام الأول إلى

تضخيم التوترات الاجتماعية في مختلف البلدان، وخصوصًا في حالات الاستقطاب السياسي المكثف، كما هو الحال أثناء استفتاء خروج بريطانيا من الاتحاد الأوروبي، أو التصويت الانفصالي الكاتالوني، أو أحداث الاحتجاجات في فرنسا.

وهناك خمسة أساليب مختلفة يمكن للدبلوماسيين الرقميين استخدامها منفصل أو مجتمعة لمواجهة التضليل الرقمي:

1. التجاهل

غالبًا ما يكون تجاهل التصيد والتضليل هو الخيار الافتراضي للدبلوماسيين الرقميين العاملين في السفارات لأسباب عديدة، حيث يمكن لهذا الأسلوب أن يبقي الحديث مُركَّزًا على الرسالة الرئيسية، وقد يمنع التصعيد من خلال حرمان المتصيدين من الاهتمام الذي يتوقون إليه، ويمكن أن يحرم القضايا المثيرة للجدل من الدعاية، وقد يعمل على حماية الدبلوماسيين الرقميين نفسيًا من الإساءة اللفظية أو الاضطراب العاطفي.

2. أسلوب التحقق

في فترة ما بعد الحقيقة، يكون التحقق من المحتوى هو الأسلوب الناجع في مواجهة سيل من البيانات المُضلِّلة، وسوء التصرّف والأخبار المزيَّفة. ويتطلب هذا التحقق من الدبلوماسيين والصحفيين والجمهور الوصول إلى معلومات دقيقة من أجل اتخاذ قرارات موثوقة، فمن

المنطقي أن تسعى السفارات إلى تصحيح التصريحات الخاطئة أو المُضلِّلة، واستخدام الأدلة الواقعية لحماية أنفسهم والسياسات التي يدعمونها من التشوهات المُتعمَّدة والسامة.

3. قلب المضامين

يمكن أن يكون استخدام الفكاهة بشكل عام والسخرية بشكل خاص فعالًا بشكل معقول في تعزيز مدى وصول الرسالة، وتحويل التحديات وتجنب التصعيد العاطفي، وتقويض مصداقية المصدر. ومن أمثلة ذلك أنّ تغريدة ساخرة للوفد المشترك لكندا في الناتو في أغسطس 2014، تسخر من تصريحات الحكومة الروسية حول دخول قواتها إلى شبه جزيرة القرم «عن طريق الخطأ»، أظهرت التزام كندا بالأمن الأوروبي وحلف الناتو، كما قوضت مصداقية الكرملين في نظر الرأي العام الغربي.

4. التشكيك

تشويه سمعة الخصم، ويكون الغرض في هذه الحالة ليس تقويض مصداقية الرسالة، بل تقويض المرسِل نفسه كي يدرك الجمهور أنّ الرسائل الواردة من مصدر معين لا يمكن الوثوق بها.

5. التعطيل

وهي تعطيل الشبكة التي يستخدمها الخصم لنشر المعلومات المضلِّلة عبر الإنترنت، وهذا يعني رسم خرائط شبكة أتباع الخصم، وتتبع الأنماط الخاصة التي يتم من خلالها نشر التضليل في جميع أنحاء

الشبكة، وتحديد حراس الشبكة الذين يمكنهم تسهيل أو عرقلة نشر المعلومات المضلِّلة. وبمجرد تحقيق ذلك، يمكن أن يحدث تعطيل شبكة المعلومات المضلِّلة من خلال استهداف حراس الشبكة بمعلومات واقعية عن القضية، وتشجيعهم على عدم الترويج «للأخبار المزيفة» والأكاذيب.

• نماذج تطبيقية لحرب الفضاء الإلكتروني

هناك صراعات إلكترونية تحركها دوافع سياسية، وتأخذ شكلًا عسكريًا يتم فيه استخدام قدرات هجومية بهدف إفساد النظم المعلوماتية، والشبكات والبنية التحتية، عن طريق استخدام أسلحة وأدوات إلكترونية. وهناك من ناحية أخرى، صراعات إلكترونية ذات طبيعة ناعمة، تدور حول الحصول على المعلومات، والتأثير في المشاعر والأفكار، وتسريب المعلومات واستخدامها عبر منصات إعلامية، بما يؤثر في طبيعة العلاقات الدولية.

فمن الصعب - كما يقال - تحريك الجبال والمحيطات، ولكن من الممكن تشغيل أو إغلاق أجزاء من الفضاء الإلكتروني بكبسة زر. ومن المؤكد أنّ تحريك الإلكترونيات عبر العالم أرخص وأسرع كثيرًا من تحريك سفن ضخمة لمسافات طويلة. الأمر الذي يسمح للجهات الفاعلة غير الحكومية والدول الصغيرة بلعب دور كبير بتكاليف زهيدة.

ويزعم (جوزيف ناي) أنّ انتشار القوة بعيدًا عن الحكومات يُعَدّ من أعظم التحولات السياسية التي طرأت على العلاقات الدولية. ويشكل الفضاء الإلكتروني مثالًا ممتازًا على ذلك، فالدول الكبيرة مثل الولايات المتحدة وروسيا وبريطانيا وفرنسا لديها قدرة أعظم من غيرها من الدول أو الجهات الفاعلة غير الحكومية في السيطرة على البحر والجو والفضاء، ولكن من غير المنطقي أنّ نتحدث عن الهيمنة في العالم السيبراني، فمن الواضح أنّ الاعتماد على الأنظمة الإلكترونية المعقدة لدعم الأنشطة العسكرية والاقتصادية يخلق نقاط ضعف جديدة في الدول الكبرى تستطيع الجهات الفاعلة غير الحكومية استغلالها.

إنّ قدرة التحكم والسيطرة من خلال الفضاء الإلكتروني وعناصر القوة الإلكترونية، ترتكز على وجود نظام متماسك يُعظِّم من القوة المتحصلة من التناغم بين القدرات التكنولوجية والسكان والاقتصاد والصناعة والقوة العسكرية وإدارة الدولة، وغيرها من العوامل التي تسهم في دعم قدرة الدولة على ممارسة الإكراه، أو الإقناع، أو ممارسة التأثير السياسي في أعمال الدول الأخرى، بغرض الوصول إلى الأهداف الوطنية، حيث أصبح للبعد التكنولوجي والاتصالي تأثير كبير في طبيعة القوة والتفاعلات في النظام الدولي (عبد الصادق، 2012: 30).

وقد بدأت الولايات المتحدة تعمل على وضع خطط معقدة تمهيدًا لهذا النوع من حروب الفضاء الإلكتروني، وبدأت قيادة حرب الفضاء

الأمريكية والأجهزة المرتبطة فيها بالعمل على وضع المخططات وتجهيز القدرات اللازمة لتحقيق الهيمنة في الفضاء الإلكتروني. ولما كانت الولايات المتحدة هي التي اخترعت الإنترنت، وهي الرائدة اليوم في مجال التجسس الإلكتروني وصنع أدوات حرب الفضاء الإلكتروني، فقد أصبحت اليوم تتعامل بقدر من الغطرسة إلى الحد الذي يجعلها تفترض أنه لا يوجد من يستطيع إخضاعها إلى حرب فضاء إلكتروني، فالولايات المتحدة تعتقد بأنّ أسلحة حرب الفضاء الإلكتروني تُعتبَر ميزة أمريكية، وأنها تقنية يجب استغلالها لتعويض ضعف انتشار القوات الأمريكية على مستوى العالم، ولتعويض التطور الهائل في الأسلحة التقليدية الموجودة في يد الخصم المحتمَل.

وتُعَد روسيا والصين من أكثر الدول تمكنًا في مجال القوة الإلكترونية، والقادرة على توفير أقصى حد من درجات الأمن الإلكتروني، وهو ما فرض على الولايات المتحدة تبني سياسات دفاعية ضد الأخطار المحتمَلة وحماية نظم المعلومات وتعزيز الأمن الإلكتروني بأبعاده المختلفة.

1. الولايات المتحدة الأمريكية

كتب العقيد الأمريكي (مايك تانكسلي Mike Tanksley) في مقال له في مجلة «تايم» عن خوض الولايات المتحدة صراعاتها المستقبلية باستخدام قدر أقل من القوة، بحيث تجبر أعداءها على الخضوع من دون

أن تطلق طلقة واحدة، وذلك باستخدام محاربي الفضاء الإلكتروني، وسيطرتهم على العدو وشلّ حركته، وتدميرهم لنظم التحكم والسيطرة، وإصدارهم أوامر زائفة لجيوش العدو. ويصف (تانكسلي) أثر استخدام هذه التكتيكات بأنه سيضع حدًا للصراع قبل أن يبدأ، من خلال زرع قنبلة منطقية تظل خاملة داخل أنظمة العدو حتى تأتي اللحظة المطلوبة فتنشط وتبدأ بالتهام بياناته، وهذه القنابل يمكن أن تهاجم أجهزة الحاسوب التي تتحكم في نظام الدفاع الجوي أو الطيران أو المصارف...الخ. وفي عام 2001 تم إنشاء مكتب خاص في البيت الأبيض لتنسيق التعامل مع مشكلة الأمن الإلكتروني، وتم نتيجة لذلك وضع الاستراتيجية الوطنية لتأمين الفضاء الإلكتروني التي وقّعها الرئيس الأمريكي (جورج دبليو بوش) عام 2003. وفي عام 2007 قام الرئيس الأمريكي الأسبق (جورج دبليو بوش) بإصدار المبادرة الوطنية الشاملة لتأمين الشبكات (PDD54)، وهي وثيقة سرية تضم الخطوات الواجب اتباعها لتعزيز الدفاعات الحكومية ضد حرب الفضاء الإلكتروني، وطالب بوش بتدبير مبلغ 50 مليار دولار على مدى خمس سنوات للمبادرة الوطنية الشاملة لتأمين الشبكات.

وتسيطر على الولايات المتحدة بشأن موضوع حرب الفضاء الإلكتروني النظرية القائلة بأنّ الفضاء الإلكتروني (نطاق) أو ساحة تدور فيها رحى الحرب، ويجب أن تهيمن عليها الولايات المتحدة. ويلاحَظ أنّ ضرورة اتخاذ الولايات المتحدة المبادرة في حرب الفضاء الإلكتروني

هي مسألة تمليها عدة عوامل منهـا: أنّ التحركـات التـي تجـري في الفضـاء الإلكتروني تتم بسرعة لم تشهدها حرب من قبل، وأنّ الفضـاء الإلكـتروني يسمح بدرجة كبيرة من المناورات العملياتية وبسرعات تقترب من سـرعة الضوء، وتتيح دائما للقادة فرصًا مختلفة للتأثير بسـرعة لـم يكـن لأحـد أن يتصـورها مـن قبـل. كمـا تلاحـظ الاسـتراتيجية أنّ المـرء إن لـم يسـارع بالتحرك فقد لا يستطيع التحرك مطلقًا؛ لأنّ الهدف الذي كـان ضـعيفًا مـن قبل قد يحلّ محله هدف آخر، وقد يتم تزويده بدفاعات جديدة دون سابق انذار، مما يجعل عمليات الفضاء الإلكتروني أقلّ فاعليـة. أي أنّ المـرء إذا انتظر الجانب الآخر ليبدأ الهجوم عليه في الفضاء الإلكتروني فقد يكتشف أنّ غريمـه في لحظـة الهجـوم نفسـها لـم يحـذف قنابلـه المنطقيـة، أو فصـل الأهداف عن مسارات الشبكة التـي أراد المـرء اسـتخدامها للوصـول إلـى هذه الأهداف (جواد، 2016: 139).

قامـت الولايـات المتحـدة الأمريكيـة في العقـد الأول مـن القـرن الحـادي والعشرين بتطوير نوع جديد من الأسلحة، وهي أسـلحة الفضـاء الإلكـتروني، وبدأت في استخدامه بصورة منهجيـة اعتمـادًا علـى تقنيـات جديـدة، وأنشـأت قيـادة عسـكرية لخـوض هـذا النـوع الجديـد مـن الحـروب (حـروب الفضـاء الإلكـتروني Cyber Space War) باسـتخدام أحـدث التقنيـات (كـلارك، 2012: 8).

وفي الوقت الذي بدأ فيه (جورج دبليو بوش) رئاسته الثانية كانت أهمية حرب الفضاء الإلكتروني قد صارت واضحة تمامًا للبنتاغون، من خلال إنشاء قيادة لحرب الفضاء الإلكتروني، تشترك فيها أفرع القوات المسلحة على أن تظل خاضعة للقيادة الاستراتيجية. وفي تشرين الأول 2009 فُتِح باب الانضمام إلى قيادة حرب الفضاء الإلكتروني الأمريكية التي تشمل عدة أفرع رئيسية في الجيش. وتولى أحد جنرالات الجيش الأمريكي رئاسة هيئة عسكرية جديدة في الولايات المتحدة الأمريكية تُعرَف بقيادة (حرب الفضاء الإلكتروني)، مهمتها استخدام تقنيات المعلومات والإنترنت كسلاح للحرب. وتقوم قيادة حرب الفضاء الإلكتروني في الولايات المتحدة الأمريكية بتجهيز ساحة حرب الفضاء الإلكتروني بما يطلق عليه القنابل المنطقية (Logic bombs) وثغرات التسلل (Trapdoors)، ووضع متفجرات افتراضية في الدول الأخرى في وقت السلم.

ودعا الرئيس الأمريكي السابق باراك أوباما أثناء حملته الانتخابية إلى وضع معايير جديدة صارمة لتوفير الأمن السيبراني، وضمان قدرة البنية الأساسية الحرجة على الصمود في مواجهة الهجمات، كما وعد بتعيين مستشار للأمن السيبراني الوطني، يكون تابعًا له مباشرة ومسؤولًا عن وضع الخطة السياسية اللازمة وتنسيق جهود الوكالة الفيدرالية. ولكن لم تكن هذه المهمة سهلة، وذلك لأن القسم الأعظم من البنية الأساسية

المطلوبة غير خاضع للسيطرة الحكومية المباشرة. وقد أوضح الرئيس باراك أوباما عام 2009 في المبادرة الوطنية الشاملة لأمن الفضاء الإلكتروني أنّ الأمن الإلكتروني هو أحد التحديات الوطنية الجادة التي تواجه الأمة الأمريكية. ووافق الرئيس أوباما عام 2009 على قبول التوصيات التي توصلت إليها مراجعة سياسة أمن الفضاء الإلكتروني، والتي تضمنت إنشاء فرع تنسيق تنفيذي لأمن الفضاء الإلكتروني، يضمن استجابة موحَّدة منظَّمة للحوادث المستقبلية لأمن الافضاء الإلكتروني، وإنشاء قوة لحماية أمن الفضاء الإلكتروني. وبنيت هذه المبادرة على المبادرة الوطنية الشاملة لأمن الفضاء الإلكتروني في عهد الرئيس (جورج دبليو بوش)، وقد ميّز الرئيس باراك أوباما أهمية الفضاء الإلكتروني، وحدد هيكلية ومصادر الأمن الإلكتروني القائم، وأعلن عن إنشاء مركز الفضاء الإلكتروني للإشراف على تهديدات الفضاء الإلكتروني المتصاعدة، وأمر بمراجعة شاملة لسياسات وهيكليات أمن الفضاء الإلكتروني.

وقبل أيام من الحملة العسكرية على ليبيا في مارس 2011 قامت الولايات المتحدة بتحريك ترسانتها الإلكترونية، وتم تخصيص 500 مليون دولار في ميزانية عام 2012 لمواجهة التهديدات الإلكترونية وتطوير أسلحة وأدوات لحرب الفضاء الإلكتروني. وفي 4 مايو 2018 رفع البنتاجون مرتبة وحدة الحرب الإلكترونية بوزارة الدفاع، وحوّلها إلى

«قيادة موحَّدة» مستقلة، وعيّن لها مديرًا جديدًا، نظرًا للأهمية المتزايدة للحرب الرقمية والهجمات الإلكترونية المتطورة، وتولى الجنرال بول ناكاسون رئاسة قيادة الأمن الإلكتروني الأمريكية، وجرى رفع وضعية هذه الوحدة إلى «قيادة موحَّدة» مستقلة، وهو تغيير حكومي وضعها لأول مرة في مصاف تسع قيادات قتالية أمريكية أخرى. ووصف مساعد وزير الدفاع باتريك شاناهان هذا التغيير بأنّه: «إقرار بأنّ هذا النوع الجديد من الحروب بلغ أعلى درجة من التطور والخطورة».

2. فيروس ستوكس نيت

انتشر العديد من المعلومات المتضاربة في شأن الفيروس المسمى (Stuxnet) الذي اكتشفته في صيف 2010 مؤسسة من روسيا البيضاء، وهو يستهدف أجهزة المراقبة من نوع SCADA (الإشراف على مراقبة واستخراج المعلومات) (Supervisory control and data Acquisition)، وخصوصًا منها مجموعات سيمنس Siemens للتنظيم والتعديل، وذلك لإلحاق أضرار كبيرة بالمنشآت التي تراقبها هذه المجموعات. وهذا الأمر لا يعدو أن يكون، حسب بعض الخبراء، تطورًا بدائيًا جدًا لبرمجيات عدائية مثل دودة ناشي Nachi التي أصابت في عام 2003 شبكات موزعات الأوراق النقدية أو دودة زوتوب Zotop التي حولت الحواسيب سنة 2005 إلى آلات خاضعة لمراقبة قراصنة دون علم أصحابها. ويرى آخرون أنّ هذا الفيروس هو آلة حرب معقَّدة جدًا

ومعزَّزة بمئات الآلاف من خطوط البرامج، وما كان يمكن أن تصنعها إلا فرق مدربة. ويستغل هذا الفيروس عدة خطوط للانتشار، وذلك شيء لم يحدث من قبل على الإطلاق، ويتوفر لهذا الفيروس نظام تخَفٍّ يجعل اكتشافه عسيرًا (بنور، 2015: 61).

ويتميز فيروس (ستوكس نيت) بقدرته على تغيير قواعد إحكام العمل بكيفية تجعله يُحدِث اضطرابات في عمل الحواسيب، ويرسل في الآن نفسه معلومات كاذبة ومطمئنة إلى قاعات المراقبة. وقد يكون قادرًا على الدخول في حالة نوم والعودة إلى النشاط والعمل من جديد إلى حدّ أن محاولات عدة أصابته أقرت أنها لا تعرف إن كانت قد أفلحت في القضاء عليه قضاء كاملًا (جواد، 2016: 135).

وجاء الهجوم الإلكتروني بفيروس (ستوكس نيت) على برنامج إيران النووي عام 2010 ليمثل نقلة مهمة في مجال تطور أسلحة الفضاء الإلكتروني. ويمثل النموذج الإيراني حالة فريدة لتحول الفضاء الإلكتروني إلى ساحة قتال بأشكال متعددة في إطار المواجهة بين الولايات المتحدة وإيران، فقد استُخدِم الفضاء الإلكتروني في شنّ هجمات تخريب للبرنامج النووي الإيراني للعمل على تعطيله، ففي 17 فبراير 2012 أعلنت الاستخبارات الإيرانية أنّ فيروس (ستوكس نت) أصاب ما يقدر بستة عشر ألف جهاز كمبيوتر (بنور، 2015: 64).

3. هجوم إستونيا عام 2007

في عام 2007 تعرضت (إستونيا) إحدى جمهوريات الاتحاد السوفييتي السابق، التي تتميز بتوافر خدمات الإنترنت فيها، وانتشار الشبكات ذات السرعات العالية، واستخدام تطبيقات الإنترنت في مجال الحياة اليومية، إلى هجوم مجموعة واسعة من الأجهزة لتعطيل خدمة الإنترنت فيها. ويتلخص هذا الهجوم بأنّه طوفان مبرمج من الحركة المُصمَّمة عبر شبكة الإنترنت بغرض تعطيل الشبكات عن العمل أو خنقها وهي موسَّعة أو منسَّقة، بمعنى أنّ آلافًا أو مئات الآلاف من أجهزة الحاسوب الموزّعة في أماكن مختلفة من العالم تُستغَل في إرسال نبضات الاستدعاء الإلكترونية إلى مجموعة من مواقع الإنترنت المستهدَفة. ويطلَق على أجهزة الحاسوب المهاجِمة لفظ (robotic network) أي شبكة مسيَّرة (مسلوبة الإدارة)، وهي مكوَّنة من مجموعة من أجهزة الحاسوب الخاضعة للتحكم عن بعد في هذه الأجهزة المستلَبة، وتتبع تعليمات تم إدخالها إلى الأجهزة دون علم أصحابها، ولا يعرف صاحب الجهاز متى استُلِب جهازه ومن قام باستلابه. وسرعان ما بدأت الشبكات المستلَبة في (إستونيا) في استهداف عناوين الأجهزة الخادمة التي تدير شبكات الاتصال الهاتفية في البلاد، ونظام التحقق من هوية مستخدمي البطاقات الائتمانية، وقد بدأ مصرف هانز بانك (Hans bank) في الترنّح، وتأثرت التجارة والاتصالات. وزعمت (إستونيا) أنّ أجهزة التحكم النهائية كانت

في روسيا، وأنّ الشيفرة الحاسوبية المُستخدَمة في هذه العملية كانت مكتوبة بالألفبائية السلافية. ومن جانبها أنكرت الحكومة الروسية باستياء شديد أنّ لها يدًا في حرب الفضاء الإلكتروني على إستونيا، كما رفضت طلبًا دبلوماسيًا رسميًا من إستونيا بمساعدتها في تعقب المعتدين على الرغم من وجود اتفاقية ثنائية بين البلدين (كلارك، 2012: 31).

وقد اتجه حلف الناتو بعد عجزه عن مواجهة الهجمات على إستونيا عام 2007 إلى تكوين وحدة للدفاع الإلكتروني مقرها (تالين) عاصمة إستونيا، كما تم تطوير المفهوم الاستراتيجي للحلف بحيث أصبح الفضاء الإلكتروني منطقة لعملياته. ومن مهامه تطوير قدراته الدفاعية الإلكترونية بما يشمل مساندة ودعم حلفائه الذين يتعرضون لهجمات إلكترونية (عبد الصادق، 2012: 33).

4. كوريا الشمالية

أرسلت كوريا الشمالية في تموز 2009 رسالة مُشفَّرة إلى 400 ألف حاسوب حول العالم وهي مُحمَّلة بفايروس للسطو على الشبكات. وتضمنت الرسالة مجموعة من التعليمات التي تجعل الحاسوب يبدأ بإرسال النبضات المطالِبة بالاتصال بقائمة من مواقع الإنترنت الخاصة بالولايات المتحدة الأمريكية وحكومة كوريا الجنوبية وعدد من الشركات الدولية، وعندما يتم تشغيل الأجهزة تنضم إلى الهجوم. وقد تعرضت المواقع الأمريكية لحِمل بلغ مليون طلب في الثانية مما أدى إلى

اختناق الأجهزة الخادمة، فتعطلت الأجهزة الخادمة للخزانة العامة والخدمة السرية وهيئة التجارة الفيدرالية ووزارة النقل وبورصة نيويورك وموقع هيئة البريد بواشنطن. ويبدو أنّ هجوم كوريا الشمالية لم يكن مجرد عدوى دودية انطلقت في غياهب الإنترنت وسُمِح لها بالانتشار، بل كان هناك من يتحكم في الهجوم ويوجّه ويُعدّل قائمة الأهداف.

وقد أعلنت كوريا الشمالية عن مخططات لإنشاء قيادة للحرب الإلكترونية بحلول عام 2012، وفي حال شنّت كوريا الشمالية ضربة إلكترونية فإنّ خيارات الرد عليها ستكون قليلة نسبيًا، فليس من الممكن تشديد العقوبات أكثر مما هي عليه اليوم، كما أنّ أي عمل عسكري غير وارد على الإطلاق، إضافة إلى أنّ احتمالات الرد بالطرقة نفسها محدودة للغاية، لأنّ كوريا الشمالية ليس لديها الكثير مما يستحق المهاجمة من جانب الولايات المتحدة أو كوريا الجنوبية (كلارك، 2012: 43).

5. الصين

عملت الصين على الاستثمار في التقنيات الجديدة، ومنها تقنية بناء الشبكات للتعامل مع ساحة حرب الفضاء الإلكتروني، وفي نهاية عقد التسعينات كان الخبراء الاستراتيجيون الصينيون قد اتفقوا على فكرة مفادها أنّ الصين يمكن أن تستخدم حرب الفضاء الإلكتروني تعويضًا عن قصورها العسكري النوعي مع الولايات المتحدة الأمريكية. وبحلول عام 2003 أعلنت الصين عن إنشاء وحدات حرب الفضاء الإلكتروني، وهاتان

الوحدتان هما المسؤولتان عن الهجوم والدفاع على شبكة الإنترنت، وفي الوقت الذي أعلنت فيه الصين عن إنشاء هذه الوحدات تعرضت الولايات المتحدة لأسوأ عملية تجسس إلكتروني أطلق عليها اسم (مطر العمالقة Titan Rain)، وتم فيها سحب ما يتراوح من 10–20 تيرا بايت من المعلومات من شبكة البنتاجون وشركة المقاولات الدفاعية (لوكهيد مارتن Lockheed Martin) وغيرها من المواقع العسكرية (Michael، 2009: 11).

وبحلول عام 2007 بدا أنّ الحكومة الصينية منخرطة في سلسلة واسعة من عمليات اختراق الشبكات الأمريكية والأوروبية، ونسخ وتصدير وإتلاف كميات كبيرة من البيانات. وقد اتهمت الولايات المتحدة الصين مرارًا وتكرارًا باختراق شبكاتها الإلكترونية، حيث اتهمتها باختراق نظم المعلومات لأقمارها الصناعية في الفضاء الخارجي، ولكنّ مسؤولي الاستخبارات الأمريكية لا يعتبرون الصين التهديد الأول للولايات المتحدة الأمريكية في مجال حرب الفضاء الإلكتروني، لأنهم يعتبرون الروس أفضل منهم، بل ويفوقون الولايات المتحدة في قدراتهم (Misha، 2011).

6. مجموعة أنونيموس Anonymous

كانت بداية الأنونيموس – وهي مجموعة من القراصنة المحترفين – عن طريق شبكة لامركزية تصرفوا فيها بشكل مجهول ومنسق نحو هدف ذاتي حرّ اتفقوا عليه، وكان غرضهم من ذلك التسلية، ولكن مع بداية عام 2008 أصبحت جماعات أنونيموس مرتبطة بشكل متزايد بالعمل الجماعي العالمي للاختراق، فقاموا بمظاهرات وأفعال أخرى في نفس السياق ضد القرصنة الرقمية من خلال مكافحة الصور المتحركة وتسجيل الجمعيات التجارية الصناعية. وكانت الأفعال المنسوبة للأنونيموس تُقام بواسطة أفراد غير معروفين يضعون مُلصق أنونيموس عليهم كشعار انتماء. وقد أثنى عليهم بعض المحللين كمقاتلين رقميين، وأدانهم آخرون بوصفهم مقاتلين حاسوبيين فوضويين. ولم يكن الأنونيموس ملتصقين بموقع إنترنت واحد، فالكثير من المواقع كانت مرتبطة معهم بشكل قوي، مما جعل لهم علامة تجارية بارزة.

وهذه المجموعة مسؤولة عن الهجمات الإلكترونية للاختراق التي طالت البنتاغون، إضافة إلى تهديدها شركة نيوز كوربوريشن بتدمير موقع الفيس بوك الخاصّ بها، وفي أكتوبر عام 2011 هدد مخترقو الأنونيموس عصابة لترويج المخدرات في المكسيك تعرف باسم لوس زيتاس، قامت بمهاجمتهم من خلال فيديو عبر الإنترنت بعد أن تم خطف أحد الأعضاء، وفي أواخر مايو 2012، وفي بداية سبتمبر 2012، تحملوا أيضًا

مسؤولية إغلاق شركة (جودادي) المؤثرة على المشاريع الصغيرة حول العالم، وفي منتصف شهر سبتمبر عام 2012 قاموا بتهديد منظمة هونكونج الحكومية التي تعرف بالمركز التعليمي الوطني عبر فيديوهات على شبكة الإنترنت.

ومن أشهر عمليات الأنونيموس الهجمة الإلكترونية على إسرائيل (أوب – إسرائيل op-Israel#)، وهي أكبر عملية قرصنة استهدفت مواقع إلكترونية إسرائيلية حساسة بلغت خسائرها حتى الآن 3 مليار دولار أميركي، بينما أوردت تقارير غير متطابقة بأنّ الخسائر قد تصل إلى 5 مليار دولار أميركي. وأعلنت المجموعة الدولية المكونة من آلاف قراصنة الكمبيوتر العرب والأجانب عن هدف الهجوم، وهو «محو إسرائيل من الإنترنت، والرد على سياساتها ضد الفلسطينيين».

يضاف إلى ذلك الفيديوهات التي قامت «الأنونيموس» بترويجها على موقع اليوتيوب ومواقع التواصل الاجتماعي، لتكشف فيها عن عملية إسقاط المواقع التابعة لجماعة الإخوان المسلمين في مصر. وكان الدافع الرئيسي لذلك هو ما وُصِف بالتهديد الذي تشكله الجماعة على الثورة المصرية، وكذلك على مصالح أخرى كالولايات المتحدة الأمريكية. وقد تمت العملية التي أطلقوا عليها اسم (Operation Egypt) في الساعة الثامنة من مساء يوم الحادي عشر من نوفمبر عام 2011 م.

الفصل الرابع

الحرب النفسية الإلكترونية

تتـأثر أفعـال وتحركـات المكونـات السياسـة في نشـاطاتها المتعـددة بالعديد من المتغيرات الكونية والتكنولوجية المتطورة، التي تتفاعل سلبًا أو إيجابًا في حركتها الصراعية في المجتمع الدولي، وهذا ما يبرز الجانب التقنـي والمعلومـاتي ضـمن الموجـات المتجـددة للتطـور التكنولـوجي والتقني كفاعل مهم في تغيير استراتيجيات العمل السياسي بشقيه العنيف والناعم، فضلًا عن أنّ الفضاء الإلكتروني المفتوح ساحة جديدة للأداء السياسي المرتبط بالهدف الاستراتيجي للدولة، وبما يعبر عن قدرتها وإجراءاتها المؤثرة على الخصم.

وقد كانت الحرب بمفهومها العسكري التقليدي إحدى أهم الوسائل المتاحة لفض الصراعات القائمة وفرض الإرادات، وفي وقت قريب تدخلت في هذه الصراعات بعض المتغيرات التي أثرت على اتجاهات السياسة في الاعتماد المطلق على الحرب المباشرة، أو الصدام المسلح كعامل فاعل لتأمين غاياتها. ومن بين تلك المتغيرات التطور الكبير الذي طرأ على وسائل الاتصال ونقل المعلومات، وهو ما جعل عالم اليوم صغيرًا إلى الحد الذي يستطيع فيه المرء أن يرى أحداثًا تقع في مختلف أنحائه لحظة وقوعها وهو جالس في بيته، مما جعل هذه الوسائل ذات تأثير كبير على تشكيل الآراء والتوجهات والقناعات، ويمكن استثمارها بأقل ما يمكن من الخسائر.

إنّ هذا التطور الكبير في وسائل الاتصال أثر بشكل ملحوظ على رؤية العديد من دول العالم، ودفعها إلى التفكير بوسائل جديدة قادرة على إحداث فعل التأثير على تشكيل الآراء والقناعات المناسبة، وتكوين الاستجابات المطلوبة التي تتوافق وواقع الحال، ومساعيها الحثيثة لتسيير مصالحها الاستراتيجية بطرق مقبولة لا تثير احتمالات المقاومة، كما يحدث عادة في التعامل مع الأساليب القديمة المتمثلة بالحرب التقليدية، وبكلفة أقلّ بالمقارنة مع الكلف الباهظة للحروب التقليدية، وسعة تدمير أقلّ بالمقارنة مع تلك الحروب (إبراهيم، 2011: 110).

ولهذا بات التعامل على المستوى النفسي يحتل الحيز الأكبر بين الأسلحة المُستخدَمة حاليًا في النظام الدولي الذي ظهر فيه فاعلون دون مستوى الدولة، وذلك للتأثير على وعي المستهدَفين. وقد أخذت فيه الحرب النفسية إطارًا أكثر شمولية، وأصبح فيها الفضاء الإلكتروني من أدواتها المعروفة والأكثر استخدامًا، وبات استخدام المعطيات الإلكترونية النفسية السرية والعلنية الوسيلة الأكثر فاعلية لإيجاد القناعات والآراء والاتجاهات التي تُسهِّل تأمين المصالح وتُعين على إدارة الصراع وتحليله.

وقد أصبحت النصوص الإلكترونية والوسائط الإعلامية المختلفة المجال الأوسع تطبيقًا في الصراعات الدولية المعاصرة، وأصبحت السيطرة على الساحات الافتراضية وخطوط الشبكة العنكبوتية والتحكم

فيها الوسيلة الأكثر فاعلية لتحقيق الأهداف المرجوة، الأمر الذي أدى إلى تعدد أشكال ووسائل حرب الفضاء الإلكتروني. وسوف يتم التركيز في هذا الفصل على مفهوم الحرب النفسية الإلكترونية ومجموعة من الأدوات والوسائل المستخدمة فيها، ومن ثم سيتناول موضوع مواقع التواصل الاجتماعي لدورها الكبير في الحرب النفسية الإلكترونية كمصدر للمعلومات أو كأداة للتعبئة السياسية والتجنيد السياسي، وستتم مناقشة موضوع الحملات الإلكترونية التي باتت من أهم الوسائل التي تُستخدَم في التعبير عن الرأي أو الاحتجاج على قضايا وسياسات معينة.

• مفهوم الحرب النفسية الإلكترونية وأدواتها

من المعروف أنّ أي تطور في الحياة ودخول أي اختراع جديد يُحدِث تغييرًا اجتماعيًا في العديد من مجالات الانشطة البشرية، فلكلّ مجتمع خصوصيته التي تميزه عن غيره من المجتمعات، وتحدد هذه الخصوصية خصائص المرحلة التي تعيشها تلك المجتمعات، فالمجتمعات الحديثة اختلفت في الكثير من الجوانب سواء على المستوى الاجتماعي أم الاقتصادي أو السياسي عن سابقتها، ومن ثم فالمؤثرات التي كانت تحدث في المجتمعات الزراعية والصناعية تختلف عن المؤثرات التي تحدث في مجتمع المعلومات، حيث تشكل التكنولوجيا المعرفة الآلية التي أصبحت تؤثر في عملية إدارة العقول كما تشكل السيطرة الثقافية، بل

إنّ اندماج ثلاث تقنيات اتصالية هي الاقمار الصناعية والكمبيوتر والنظام الرقمي أدى إلى تغيير سريع في الثقافات وانهيار ثقافات أخرى.

يتمثل نمط الاستخدام «الصلب» للقوة الإلكترونية في استخدام أدواتها للقيام بعمل تخريبي، عبر قطع كابلات الاتصالات، أو تدمير أنظمة الاتصالات، أو الأقمار الصناعية، أو استخدام الأسلحة الإلكترونية المتقدمة كالفيروسات في تدمير الأنظمة المعلوماتية لمنشآت حيوية بشكل يؤثر في وظيفتها، ويهدد أمن الدولة والسكان. أما نمط «القوة الناعمة» فيتعلق بإدارة العمليات النفسية، والتأثير في الرأي العام، وفي عمل أجهزة الاستخبارات الدولية، فقد وفر الفضاء الإلكتروني سيلًا من المعلومات لا يقتصر على وجهة النظر الرسمية للدول والحكومات، بل أصبح للأفراد دور في إنتاج المعلومات وترويجها، وشكّل ذلك ثورة معلوماتية هائلة لا حدود لها، عكفت أجهزة الاستخبارات الكبرى على متابعتها وتوظيف نتائجها (عبد الصادق، 2012: 31).

وهناك الكثير من الأساليب التي تعتمدها القوة الناعمة، وهي أكثر خطورة من القوى الصلبة لأنّ الثانية تنشط في المواجهات المباشرة فقط، لكنّ الأولى تنشط في كلّ وقت وحين، ومن أهم وسائلها: الرسائل الإلكترونية، والحملات الإعلامية، والمعارك الكلامية في الإذاعات الموجَّهة والدولية، والبث الفضائي وما يشكله من غزو ثقافي وإلكتروني، والاكتساح الإعلامي بما يسببه من إشاعة لثقافة العنف في المجتمعات من

خـــلال الـــبرامج والافـــلام والمسلســـلات الموجَّهـــة ذات الطبيعـــة الاستهلاكية.

ففي عالم يسوده الصراع وعدم توازن القوى يتم اللجوء إلى أساليب الحرب النفسية واستخدامها إلكترونيًا، ولكنّ هذه الاستخدامات لا تأتي من فراغ، بل تكون مبنية على أسس ومعايير علمية وتجارب مختبرية، فالحرب المعلوماتية تتم على مستوى رمزي ولكلّ أطراف الصراع، ولا بدّ من أن تكون لها الطريقة العلمية التي تعتمدها في التوجه إلى الجمهور المستهدَف.

وهناك العديد من المحاولات في تحديد مفاهيم تقترب من مفهوم الحرب النفسية الإلكترونية، ونجد عددًا كبيرًا من التعريفات لمفهوم الحرب النفسية والدعاية في الكثير من الأدبيات الغربية والعربية، منها – مثلًا – تعريف عالم الاجتماع الفرنسي «جاك إيلوك» للدعاية بأنها «مجموعة من الوسائل يتم توظيفها بواسطة جماعة معيَّنة منظَّمة، تريد تحقيق مشاركة نشيطة أو سلبية، في عمل معين تقوم به تجاه جماهير موحدة سيكولوجيًا من خلال التلاعب أو التصنيع السيكولوجي»، أما في مجال الفضاء الإلكتروني فيمكن تعريف الحرب النفسية الإلكترونية بأنها أي نشاط اتصالي أو هجوم إلكتروني يمارس ضد جمهور ما باستخدام تكنولوجيا الاتصال الحديثة من بث فضائي وإنترنت بخدماته المتنوعة، بهدف التأثير وتغيير اتجاهات ومواقف الجمهور المستهدَف، من خلال

ما تبثه من معلومات مضخَّمة أو بث سيل ضخم من المعلومات تؤدي إلى إرباكه وتشويشه.

ومن أهم أدوات الحرب النفسية الإلكترونية: الدعاية عبر الإنترنت، والفضائيات التلفزيونية، والهندسة الاجتماعية. ويمكن تفصيل هذه الأدوات على النحو التالي:

- **الدعاية عبر الإنترنت**

ساهمت الثورة الاتصالية والتكنولوجية الجديدة لوسائل الإعلام الإلكترونية، وعلى رأسها الإنترنت، في ظهور فضاء عام اجتماعي جديد، يعتمد على أسس يكون فيها الرأي العام حرًا في حركة المعلومات وتبادل الأفكار بين جميع مكونات النظام الدولي، فالإنترنت تقدم إمكانيات جديدة مقارنة بوسائل الإعلام التقليدية، فهي تجعل من السهل نشر المعلومات بين الأفراد.

ويمكن إجمال العناصر الرئيسية التي تشتمل عليها الإنترنت بما يلي:

1. مستخدمو الشبكة باختلاف مشاربهم وأذواقهم وآرائهم وحاجاتهم الاتصالية والإعلامية التي تدفعهم لاستخدام الشبكة.
2. الخدمات المُقدَّمة من الشبكة: وهي تتنوع بتنوع المعارف والعلوم، وحاجات مستخدمي الشبكة، والحاجات الإنسانية، ومنها البريد الإلكتروني، والمجموعات الإخبارية، والمنتديات، والدردشة.

3. التقنيات المُستخدَمة في الشبكة: وهي تنقسم إلى قسمين، هما: الأجهزة الحاسوبية المُستخدَمة للارتباط بالشبكة Hardware، والبرامج اللازمة للارتباط بالشبكة Software.

وقد أثبتت هذه التقنيات فعالية الإنترنت كسلاح دعائي في الحرب النفسية، وأعطت الصراع بعدًا آخر من خلال التقنيات الدعائية الكثيفة التي استُخدِمت في العديد من الحروب، والتي لجأت إليها الأطراف المتصارعة كنوع من الأسلحة المكمِّلة التي تهدف إلى التأثير في العدو وبث البلبلة في صفوفه واختراقه، وقد عُرِفت هذه الحروب بالحروب السيكولوجية الإلكترونية أو الحروب النفسية الإلكترونية.

ويتطلب العمل الدعائي على الإنترنت استراتيجية ذكية تكمن في وضع قائمة بأسماء الشخصيات الفاعلة، وإغراق صناديقها الإلكترونية بالرسائل الدعائية من كلّ نوع. ومن أبرز الأسلحة المستخدَمة في الحرب النفسية الإلكترونية التضخيم المعلوماتي وإغراق الخصم بالمعلومات، حتى يصعب عليه التمييز بين الخطأ والصواب. وهناك أسلوب آخر هو التجهيل والتضليل من خلال بث بعض المعلومات بأساليب معينة تعمل على دفع الجمهور لاتخاذ ردود أفعال ومواقف طبقًا لما تريده تلك القوى المسيطرة على عملية تدفق الأخبار، وتؤدي إلى زيادة الخوف لدى الجماهير والخضوع لسياسة الخصم.

وقد مكّنت شبكة الإنترنت منظمات الحركة الاجتماعية وشبكات الناشطين من صياغة أطر مشتركة للمعنى، والقيام بأعمال مشتركة. وهناك أربعة أسباب جعلت للأنترنت أهمية كبيرة في هذا المجال (بيلي وآخرون، 2009: 152):

1. التنسيق بين شبكات الحركات الاجتماعية عبر الحدود دون الحاجة إلى تخطي الشكل التنظيمي الهرمي.
2. إحداث تأثير مرتفع دون الحاجة إلى قدر كبير من الموارد.
3. ساعدت المنظمات على الاحتفاظ بالسيطرة التحريرية على المحتوى (المضمون) والاتصال الخارجي.
4. مكّنت المنظمات من تفادي سيطرة الدولة ورقابتها، والتواصل في بيئة آمنة.

ويعتمد النسق المفاهيمي للحرب النفسية الإلكترونية على نظرية الموجة الثالثة التي جاء بها الباحث الأمريكي «إلفن توفلر»، وتذهب هذه النظرية إلى افتراض مرور العالم بثلاث موجات من الثورات التقنية، جاعلة تقنية المعلومات هي الموجة الثالثة التي أدت إلى تغييرات حاسمة في الأنساق والمفاهيم السائدة في ميدان الاتصال والإعلام، كما أحدثت تغييرات جوهرية في طبيعة الآليات المعرفية والإعلامية التي يمارسها الإنسان المعاصر بعد ظهور خدمات الوسائط المتعددة والتضخم الكبير في حجم البيانات والمعلومات. أدت كلّ هذه الامور إلى اهتمام عدد كبير

من الباحثين بمفاهيم هذه النظرية، ومنهم المفكر الأمريكي «جون بويد» الذي ذهب إلى تأكيد وجود حلقة تأثيرية تتألف مادتها من أربعة عناصر رئيسية يرمز إليها بالرمز (OODA)، وتمارَس في الذهن البشري وهي: يراقب (observe)، يوجه (orient)، يقرر (Decide)، يفعل (Act). وتسهم نشاطات الحرب النفسية المعلوماتية في إحداث خلل في حلقة (OODA) لدى الآخر، بقصد إحداث تأخير في نمطها الدوري، وتعمل في الوقت ذاته على تحسين النمط الدوري لذاتية أخرى، فتضمن بذلك تفوقًا ملموسًا للجهة التي تمارس هذا النمط من النشاط الدعائي (إبراهيم، 2011: 118).

ومن أهم أدوات الرأي والتعبير عبر الإنترنت:

1. التجمعات الافتراضية: وهي عبارة عن مواقع على شبكة الإنترنت تمثل نقطة التقاء لمجموعة من الأشخاص، يتواصلون معًا من خلالها باستخدام نظم القوائم البريدية أو التراسل الفوري والمحادثة والحوارات المطولة، ويجمعهم اهتمام مشترك إزاء قضية ما.
2. استطلاعات الرأي الإلكترونية: التي أصبحت مادة دسمة في الكثير من المواقع على شبكة الإنترنت، والتي تهدف إمّا لاستطلاع رأي زوار الموقع تجاه موقف معين، أو محاولة بناء رأي تجاه قضية ما.

3. آلية التصويت والانتخابات: يُستخدَم الإنترنت في عملية التصويت في الانتخابات، بالإضافة إلى الأدوات الأخرى التي تساعد في إعداد الجداول الانتخابية وقواعد بيانات الناخبين وفرز الأصوات وإعلان النتائج.
4. مواقع الإنترنت الخاصة: أدت سهولة إنشاء موقع إلكتروني على شبكة الإنترنت إلى اتجاه الأفراد أو المنظمات أو الأحزاب السياسية أو منظمات المجتمع المدني إلى إنشاء مواقع خاصة تعرض لقضايا معينة. وعلى سبيل المثال، تُعَدّ شبكة المعلومات الدولية من أبرز الأدوات التي استخدمت في الحرب على العراق، لتسريبها كميات من المعلومات حول الحرب، حيث بلغ عدد المواقع التي ظهرت في هذه الفترة 884056 موقعًا، إضافة إلى دور البريد الإلكتروني في تنظيم المظاهرات ضد هذه الحرب آنذاك.
5. مواقع الشبكات الاجتماعية: وهي تلك المواقع التي تتيح فرصة التعارف والاتصال بين عدد كبير من الأفراد على مستوى العالم، كما يتم إنشاء مجموعات يمكن أن تجتذب إليها المزيد من الأفراد، وتتميز تلك المواقع بسرعة تناقل المعلومات والصور، وخاصة مقاطع الفيديو، وذلك في موقع فيس بوك وموقع تويتر.

وقد أثبتت الدعاية عبر الإنترنت أنّ الدولة أسقطت المفاهيم السياسية في أذهان الشعب عبر أساليب التضليل الدعائي، وتوظيف المقررات

الأيديولوجية من خلال الإعلان التضليلي، كما أثبتت أيضًا أنّ وسائل الإعلام لا بدّ أن تشكل البوتقة لنشر مبادئ أصحابها الأيديولوجية – أيًّا كانت هذه الأيديولوجية سياسية أو اقتصادية أو ثقافية – ونزعتهم الإثنية أو القومية أو المذهبية، كما كشفت شبكة الإنترنت أنّ الكلام عن الحيادية الإعلامية وحمايتها ما هو إلا وسيلة لإقناع الجماهير بصحة المعلومات الصادرة عن الوسائل الإعلامية التي تخفي في طياتها ما يغسل العقول ويزلزل العقائد والأفكار.

فالحرب النفسية الإلكترونية يقصد بها استخدام وسائل الإعلام الحديثة وخدمات الإنترنت في بث رسائل وأفكار وتوجهات معينة، بهدف التأثير على الجماهير والجيوش وصناع القرار. ومن أبرز الأمثلة التي تم فيها استخدام أساليب تكنولوجية لممارسة الحرب النفسية قيام القوات الأميركية إبان حرب الخليج الثانية 2003، باختراق الشبكة العسكرية ذات الدوائر المغلقة الخاصة بالجيش العراقي، وإرسال رسائل من القيادة الأميركية الوسطى إلى الضباط والجنود العراقيين عبر البريد الإلكتروني تعلن فيها غزو العراق في المستقبل القريب، وتؤكد أن الهدف هو إزاحة الرئيس العراقي صدام حسين وابنيه من دون إصابة الجنود العراقيين. وطالبت هذه الرسائل القادة بأن يضعوا المدرعات والدبابات التي تحت إمرتهم في صورة تشكيل، وطلبت منهم أن يتركوها ويذهبوا إلى بيوتهم، مما يسهل على القوات الأميركية إصابة الأهداف. وقد وجدت القوات

الأميركية عند ضرب العراق بعض الوحدات وقد اصطفت ودباباتها بانتظام أمام قواعدها، مما سمح للطائرات الأميركية بقصفها قصفًا محكمًا (خليفة، 2017: 19).

- **الفضائيات التلفزيونية**

تُعَدّ وسائل الإعلام بشكل عام من الأدوات الفاعلة والمهمة في المجال السياسي، فهي لا تقوم فقط بنقل الرسائل والمعلومات من المؤسسات السياسية إلى الجمهور، بل تحول هذه المعلومات من خلال مجموعة متنوعة من العمليات الخاصة بصناعة الأخبار لتحقيق أهداف وغايات محددة، حيث تُعَدّ العلاقة بين وسائل الإعلام والعملية السياسية علاقة جدلية، إذ إن وسائل الإعلام تعمل على نقل وتحليل النشاط السياسي، ولكنها تُعَدّ في الوقت نفسه جزءًا من العملية السياسية، باعتبارها من المصادر المتاحة أمام السياسيين وقادة الرأي للحصول على المعلومات وتَلَقِّي ردود أفعال الجمهور نحو سياستهم وقراراتهم ومواقفهم، مما يساعد على صنع القرار السياسي، فضلًا عن اعتماد الجمهور عليها في تكوين اعتقاداته واتجاهاته ومواقفه المختلفة إزاء الأحداث والسياسات التي تقع داخل الواقع المحيط به، وما يترتب عليها من سلوكيات وردود أفعال إزاء هذه الأحداث.

وقد استثمرت العديد من القوى والجماعات عصر المعلومات في تغيير استراتيجيات الحرب النفسية وصيغتها، بتسخير هذه التقنيات لتحقيق الأهداف بصورة أكثر عمقًا وسرعة، فأصبحت التغطية التلفزيونية في الفضائيات إحدى أهم أدوات الحرب النفسية الإلكترونية، واختُصِر زمن الحروب التقليدية في الوصول إلى الأهداف بزرع الهزيمة في نفس المقابل قبل بدء القتال، فاتخذت أساليب التهديد والخداع بهدف القضاء على روح المقاومة وتحطيم معنويات الشعوب (سنو، 2006: 71).

ومن أبرز الشبكات التلفزيونية التي نشطت في هذا المجال شبكة (CNN) حيث انفردت بنقل التغطية الحية المباشرة للحرب على العراق عام 2003، وكانت المصدر شبه الوحيد لبث الرسائل على مدار الساعة، ومن ثم أصبحت نموذجًا يُقتدى به في العديد من القنوات الإخبارية العربية المتخصصة (العبد، 2009: 40).

وقد أشار بطرس غالي عند توليه منصب الأمين العام للأمم المتحدة إلى أنّ قناة (CNN) هي العنصر السادس عشر في مجلس الأمن، وذلك لخطورة الدور الذي يمكن أن تلعبه وسائل الإعلام في تشكيل السياسات الدولية وقرارات الأمم المتحدة.

وأصبحت القنوات الفضائية من أكثر الوسائط الإعلامية ملاءمة لتحقيق أهداف الحرب النفسية الإلكترونية، وذلك لأنها تبث مادتها على مساحات واسعة، ويمكن من خلالها شحن الخطاب الإعلامي المحايد

بمادة تخدم الأهداف التي تسعى إليها جهات بعينها، حيث بدأ الإعلام يمارس عبر القنوات الفضائية نوعًا جديدًا من الدبلوماسية أُطلِقت عليها تسمية الدبلوماسية الشعبية، وتتم هذه الدبلوماسية عبر التواصل الإعلامي مع الشعب لضمان التأثير، وانعكاس ذلك التأثير على الرأي السياسي لصناع القرار داخل حدود البلاد.

- **الهندسة الاجتماعية**

أصبحت المعرفة في الوقت الحاضر متاحة على نحو لم يسبق له مثيل في التاريخ الإنساني، وبقوالب تقنية ميسرة وأساليب اتصالات جماهيرية. وثمة من يؤكد أن كلّ شيء نسميه معرفة قد أصبح مُرقّمًا digitized، ويمكن النفاذ إليه accessible من الجميع ومفهرَسًا تمامًا، ويمكن البحث عنه searchable بسهولة لجميع رواد الإنترنت.

وقد جاء مفهوم الهندسة الاجتماعية (Social Engineering) كفرع من فروع التكنولوجيا الناعمة (Soft Technology)، وامتدادًا طبيعيًا لعلوم الإعلام والاتصال نحو مجال الذكاء الاقتصادي أو التنافسي، فهي مزيج معقد من العلوم وعلم النفس والفن، ونستطيع تعريفها بأنها (أي فعل يؤثر على شخص كي يقوم بعمل أو يتخذ إجراء لا يكون بالضرورة في صالحه مثل الإفضاء بمعلومات سرية أو التصويت لصالح مرشح في انتخابات)، وهي بصفة عامة مجموعة من الأساليب والتقنيات ذات منهج

ترابطـي يسـتند إلـى التـأثير (Influence) والخـداع (Super Cherie) والتلاعب (Manipulation) للحصول على معلومات شخصية سرية أو الوصول إلى نظام معلومات. ومن أقرب التعريفات لمفهوم الهندسة الاجتماعية أنها استخدام المهاجم لحيل نفسية كي يخدع مستخدمي الحاسوب، ليمكنوه من الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها (أحمد، 2014: 22).

وعندما نتحدث عن عمليات القرصنة والاختراق الإلكتروني تتحوّل الأفكار نحو المحافظة على الأجهزة بأحدث برمجيات مكافحة الفيروسات والقرصنة وحمايتها من البرمجيات الخبيثة، ولكن مع أهمية ذلك كلّه فإنّه لا يمثل سوى جانب من الموضوع، وذلك لأنّ الجانب الآخر الأكثر أهمية هو العنصر البشري، فحتى لو ابتكر مطورو النظم الأمنية نظامًا معصومًا من البرمجيات الخبيثة ولا يمكن اختراقه، فإنّ هذا النظام سيظل مع ذلك مرهونًا بطريقة تعاطي المستخدِم معه. ولأنَّ كل شيء يتمحور حول المستخدِم يعتمد الكثير من المخترقين والقراصنة حول العالم على العنصر البشري فقط (المستخدِم) لاختراق الأجهزة، وهو ما بات يعرف بالهندسة الاجتماعية.

فالهندسة الاجتماعية تُعنَى باكتساب المعلومات الحساسة، أو ميزات الوصول غير المناسبة، من خلال إقامة علاقة ثقة غير ملائِمة مع مستخدمي الشبكة العنكبوتية، وهي فن انتقاء الأفراد ليفعلوا أشياء ما

كانوا ليفعلوها في الوضع الطبيعي، والهدف هو خداع شخص ما لتقديم معلومات قيمة، أو الوصول إلى المعلومات، ويركز هذا العمل على الطبيعة البشرية مثل الرغبة في المساعدة، أو الرغبة في الثقة بالآخرين، والخوف من الوقوع في المشاكل. ومؤشر الهندسة الاجتماعية الناجحة هو الحصول على المعلومات دون إثارة الشكوك، إذ يعتقد غالبية الناس أنّ الدخول إلى الحاسب يتطلب شخصًا محترفًا من الناحية الفنيّة، ولكنّ عددًا من الدخلاء تمكنوا نتيجة التدفق المعلوماتي الكبير من استغلال هذه المعلومات، والواقع أنّ الهندسة الاجتماعية تؤدي إلى خرق أمن المعلومات (Tims، 2001: 1).

فالمهندس الاجتماعي ليس ممثلًا جيدًا وحسب، بل هو شخص يتمتع بحس عالٍ من الفراسة والمقدرة على معرفة الحيل التي من الممكن أن تنطلي على الشخص الذي يتعامل معه، فعندما تجتمع لدى المهاجم الخبرة التقنية مع مهارات الهندسة الاجتماعية يصبح من السهل عليه اختراق أي شبكة والوصول إلى المعلومات المطلوبة.

إنّ الهندسة الاجتماعية القائمة على أساس تقني تحتوي العديد من التقنيات التي تساعد المهاجمين للوصول إلى المعلومات، ومن أمثلة ذلك (البداينة، 2002: 243):

1. النوافذ النازلة أو المنبثقة (Popup Window): يظهر على شاشة الحاسوب أحيانًا نافذة تُعلِم المستخدم بأنه فقد الاتصال مع

الإنترنت مثلا، وأنّ عليه الدخول مرة أخرى عن طريق (كتابة اسم المستخدم وكلمة المرور)، ويكون هناك برنامج قد تم تحميله لينقل معلومات المستخدم ويرسلها إلى حاسب المخترِق.

2. مرفق (ملحق) البريد (Mail Attachment): ويمكن إخفاء البرامج في ملحقات البريد الإلكتروني، والتي يمكنها أن تنشر الفيروس وتدمر الشبكات.

3. بريد القمامة (Spam): ورسائل السلة (Chain Letters)، والخداع (Hoaxes)، وكلّها تعتمد على الهندسة الاجتماعية في الانتشار.

4. ويمكن أن نذكر مواقع التواصل الاجتماعي التي أصبحت مصدرًا أساسيًا للمعلومات الشخصية والعائلية، حيث ينشر الكثير من الناس لحظات هامة من حياتهم، فيعلم الجميع ومنهم الأشرار والمحتالون أدق التفاصيل عن تحركات ضحاياهم، وعن عائلاتهم وأبنائهم، وعن مشتهياتهم ومشاريعهم، الأمر الذي يسهل استراتيجية الهجوم من استدراج واختراق واحتيال.

• مواقع التواصل الاجتماعي

ظهرت ضرورة الاهتمام بأمن الفضاء الإلكتروني بسبب الاستخدام الكبير لتكنولوجيا المعلومات في عمل العديد من المرافق الحيوية، مما يعرضها لخطر الهجمات الإلكترونية، كما شاع استخدام الفاعلين من غير الدول للفضاء الإلكتروني الذي يتعدى كلّ الحدود لتحقيق أهدافهم، مما كان له أثر سلبي في سيادة الدولة، ثم برزت إشكاليات تعامل الدول مع شركات التكنولوجيا متعددة الجنسيات، مثل مواقع الشبكات الاجتماعية كالفيس بوك، وتويتر، واليوتيوب التي أصبحت بمثابة فاعلين دوليين.

ويكمن النظر إلى التغير السياسي والاجتماعي برؤية (حتمية التحول في مسارين ، أولهما: ما يعرف (بالحتمية التقنية) Technological Determinism، وثانيهما: ما يعرف (بالحتمية الاجتماعية) Social Determinism، وإنّ لكلٍّ من المسارين وجهات نظر تدعم تفسيره، إلا أنّ التفسير الذي قدمه بعض المفكرين في اختلاف معدل التغير في كل من الثقافة المادية واللامادية نتيجة التأثير التقني في المجتمعات، يُعَدّ الأساس في التحليل الاجتماعي لتقنية الاتصال، مع احتمال حدوث تصادم بين التغير التقني والتغير الثقافي، ويترتب عليه خلل وظيفي مما يؤثر في تفكير أفراد المجتمع، وتتوتر القيم والإيديولوجيات السائدة (رحومة، 2007: 75).

وأمام عجز الأحزاب السياسية وجمعيات المجتمع المدني عن أداء أدوارها المتمثلة في التعبئة بسبب الأنظمة الحاكمة من جهة، وغياب الديموقراطية الداخلية في معظمها من جهة أخرى، وتحولها إلى كائنات ذات أهداف آنية من جهة ثالثة، عم نفور المواطنين منها، لذلك فإنّ الوسائط الحديثة المتمثلة في الفضاء الرقمي استطاعت أن تحلّ محلها، إذ لعبت دورًا أساسيًا في الحراك السياسي والاجتماعي الذي شهدته المنطقة العربية مع الانتفاضات الشعبية، وأسهمت بشكل كبير في نقل الوقائع الميدانية بشكل مباشر، وكذلك في تعبئة المحتجين وتنظيمهم عن طريق تسهيل التواصل فيما بينهم. ولم يكن مستغربًا أن يكون الشباب في طليعة المحتجين، لأنهم الكتلة السكانية الأكبر في المجتمعات العربية، والأكثر شعورًا بالحرمان النسبي، والأكثر قدرة على التواصل والحركة.

ويضاف إلى ذلك تسخير الجماعات الإرهابية الشبكة الرقميّة والفضائيات لأغراضها الدعائية، منذ شرع تنظيم القاعدة قبل نحو عقد من الزمن في بث بياناته عبر الإنترنت وبعض القنوات التلفزيونية العربية والعالمية، حتى برز في السنوات الخمس الأخيرة نشاط «رقمي» فعّال للجماعات المتطرفة، لتسويق بياناتها وصور فعالياتها عبر مواقع التواصل الاجتماعي، وخصوصًا «فيسبوك» و«تويتر»، في سعيها لتعزيز استراتيجية لا تكتفي بنشر ثقافتها المتطرفة والتكفيرية فحسب، بل إلى شنّ حرب نفسية للتأثير في الخصوم، والسعي إلى استقطاب الشباب للتطوّع في

صفوفها، والقتال في البلدان التي تحارب فيها مثل أفغانستان والعراق وسورية واليمن ودول أخرى.

وقد أدى الانتشار الهائل في استخدام مواقع التواصل الاجتماعي إلى إحداث «ثورة كبرى» تركت تأثيراتها في كافة جوانب الحياة، ومن بينها الأمن الوطني للدول الذي أصبح يواجه تحديات وتهديدات جديدة، بحيث توسع مفهوم الأمن الوطني ذاته ليتجاوز نطاق مواجهة التهديدات العسكرية وضمان حماية الوطن ووحدته وسلامة أراضيه وسيادته، إلى مجالات أخرى تشمل الاستقرار السياسي والاقتصادي والانسجام الاجتماعي وسلامة البيئة، ففي عام 2011، أعلنت وكالة مشاريع البحوث الدفاعية المتطورة (DARPA) عن برنامج لاستخدام مواقع التواصل الاجتماعي في تحقيق التواصل الاستراتيجي، من خلال تحسين فهم وزارة الدفاع لما يجري على مواقع التواصل الاجتماعي في الوقت الحقيقي له، وخصوصًا في المناطق التي تنتشر فيها قوات أمريكية، فضلًا عن قيام وزارة الدفاع الأمريكية باستخدام مواقع التواصل في بث رسائل إعلامية تخدم مصالحها الاستراتيجية (خليفة، 2017: 26).

- **مفهوم مواقع التواصل الاجتماعي**

إنّ مفهوم (مواقع التواصل الاجتماعي) مثير للجدل، ونظرًا لتداخل الآراء والاتجاهات في دراسته عكس هذا المفهوم التطور التقني الذي طرأ

على استخدام التكنولوجيا، وأُطلِق على كلّ ما يمكن استخدامه من قبل الأفراد والجماعات على الشبكة العنكبوتية العملاقة، فهناك الإعلام الاجتماعي، وهو المحتوى الإعلامي الذي يتميز بالطابع الشخصي، والمتناقَل بين طرفين أحدهما مرسل والآخر مستقبل عبر وسيلة شبكة اجتماعية، مع حرية الرسالة للمرسل وحرية التجاوب معها للمستقبل.

ويشير المفهوم أيضًا إلى الطرق الجديدة للاتصال في البيئة الرقمية بما يسمح للمجموعات الأصغر من الناس بإمكانية الالتقاء والتجمع على الإنترنت، وتبادل المنافع والمعلومات، وهي بيئة تسمح للأفراد والمجموعات بإسماع صوتهم وصوت مجتمعاتهم إلى العالم أجمع. ويمكن تعريف مواقع التواصل الاجتماعي أيضًا بأنّها منظومة من الشبكات الإلكترونية التي تسمح للمشترك فيها بإنشاء موقع خاص به، ومن ثم ربطه عن طريق نظام اجتماعي إلكتروني مع أعضاء آخرين لديهم الاهتمامات والهوايات نفسها (راضي، 2003: 23).

فالإعلام الجديد يُعرَّف إجرائيا بأنه: أنواع الإعلام الرقمي الذي يُقدّم في شكل رقمي وتفاعلي، ويعتمد على اندماج النص والصورة والفيديو والصوت، فضلًا عن استخدام الكمبيوتر كآلية رئيسة له في عملية الإنتاج والعرض، أما التفاعلية فهي تمثل الفارق الرئيس الذي يميزه وهي أهم سماته. ويمكن تقسيم مواقع التواصل الاجتماعي بالاعتماد على التعريفات السابقة إلى الأقسام الآتية:

1. شبكة الإنترنت ONLINE: وتطبيقاتها مثل الفيس بوك، وتويتر، واليوتيوب، والمدونات، ومواقع الدردشة، والبريد الإلكتروني.. فهي بالنسبة للإعلام تمثل المنظومة الرابعة التي تضاف إلى المنظومات الكلاسيكية الثلاث.
2. تطبيقات قائمة على الأدوات المحمولة المختلفة، ومنها أجهزة الهاتف الذكية والمساعِدات الرقمية الشخصية وغيرها. وتُعَدّ الأجهزة المحمولة منظومة خامسة في طور التشكل.
3. أنواع قائمة على منصة الوسائل التقليدية مثل الراديو والتلفزيون (مواقع التواصل الاجتماعي للقنوات والإذاعات والبرامج) التي أضيفت إليها ميزات مثل التفاعلية والرقمية والاستجابة للطلب.

ويمكن أن نخلص إلى الاتفاق على أنّ مواقع التواصل الاجتماعي تشير إلى حالة من التنوع في الأشكال والتكنولوجيا والخصائص التي حملتها الوسائل المستحدثة عن التقليدية، ولا سيما فيما يتعلق بإعلاء حالات مثل الفردية Individuality والتخصيص Customization، وهاتان الحالتان تأتيان نتيجة لميزة رئيسة هي التفاعلية، فإذا كان الإعلام الجماهيري واسع النطاق، وهو بهذه الصفة اسمه إعلام القرن العشرين، فإنّ الإعلام الشخصي والفردي هو إعلام القرن الجديد (الحادي والعشرين)، وما ينتج عن ذلك من تغيير انقلابي للنموذج الاتصالي الموروث بما يسمح للفرد العادي بإيصال رسالته إلى من يريد في الوقت

الذي يريد، وبطريقة واسعة الاتجاهات وليس من أعلى إلى أسفل وفق النموذج الاتصالي التقليدي، فضلًا عن تبني هذه المواقع تطبيقات الواقع الافتراضي، وتحقيقه لميزات الفردية والتخصيص، وتجاوزه لمفهوم الدولة الوطنية والحدود الدولية.

إنّ تأثير تكنولوجيات الاتصال على الحياة اليومية جعل من المجتمعات المحلية مجتمعات لا تتشكل فقط في المساحات الجغرافية المحددة بل أيضًا في الفضاء الإلكتروني، وتسمى (المجتمعات الافتراضية)، حيث يتسم المجتمع الافتراضي بالسمات التالية (الراوي، 2012: 100):

1. المرونة وانهيار فكرة المرجعية بمعناها التقليدي، فالمجتمع الافتراضي لا يتحدد بالجغرافيا بل بالاهتمامات المشتركة التي تجمع معًا أشخاصًا لم يعرف كلٌّ منهم الآخر بالضرورة قبل الالتقاء إلكترونيًا.
2. لم تعد الحدود الجغرافية تلعب دورًا في تشكيل المجتمعات الافتراضية، فهي مجتمعات لا تنام، ويستطيع المرء أن يجد من يتواصل معه في المجتمعات الافتراضية على مدار الساعة.
3. إنها فضاءات رحبة مفتوحة للتمرد والثورة، بداية من التمرد على الخجل والانطواء، وانتهاء بالثورة على الأنظمة السياسية.

4. تتسم المجتمعات الافتراضية بدرجة عالية من اللامركزية، وتنتهي بالتدرج إلى تفكيك مفهوم الهوية التقليدي. ولا يقتصر تفكيك الهوية على الهوية الوطنية أو القومية، بل يتجاوزها إلى الهوية الشخصية، لأنّ من يرتادونها في أحيان كثيرة يدخلون بأسماء مستعارة ووجوه ليست وجوههم، وبعضهم له أكثر من حساب.

وقد ارتكزت البحوث العلمية حول وسائل الاتصال الحديثة على نموذجين تفسيريين، يتمثل الأول في الحتمية التكنولوجية، وينطلق من قناعة بأنّ قوة التكنولوجيا هي وحدها المالكة لقوة التغيير في الواقع السياسي والاجتماعي. والنظرة التفاؤلية للتكنولوجيا تهلّل لهذا التغيير، وتراه رمزًا لتقدم البشرية، وعاملًا مهمًا لتجاوز إخفاقها في مجال الاتصال الديمقراطي والشامل الذي تتقاسمه البشرية. ويتمثل النموذج التفسيري الثاني في النظرة التشاؤمية التي ترى التكنولوجيا وسيلة للهيمنة على الشعوب المستضعَفة، والسيطرة على الفرد، إذ تقتحم حياته الشخصية، وتفكك علاقاته الاجتماعية (بيلي، كامتريس، نيكوكاربتيير، 2009: 24).

- **الفئات المُستخدَمة لمواقع التواصل الاجتماعي**

تمت إزالة الحدود وتأجيج العديد من الصراعات السياسية عن طريق مواقع التواصل الاجتماعي. ولعلّ أهم إنجاز في مواقع التواصل الاجتماعي هو الاهتمام بحق التعبير، مما أدى إلى استثارة غضب الكثير

من الحكومات التي أصبحت تضع في حساباتها هذه الوسيلة، فتداول الأحداث ذات التوجه السياسي أرغم بعض الحكومات على اتخاذ قرارات أو التراجع عن قرارات بسبب الاحتجاج الجماهيري. ويوجد أصناف لمستعملي مواقع التواصل الاجتماعي من المتلقين أو الجمهور:

الصنف الأول: وتمثله الطبقات الشعبية المُهمَّشَة، والذين يستعملون في العادة الإشاعات والنكت الشعبية والسياسية كإعلام بديل، لما يوفره لهم من الحصانة وعدم المساءلة القانونية، لأن عملية تناقل النكت والإشاعات لا تتضمن اسم منتجيها، فضلًا عن إمكانية تحويرها من متقبّل إلى آخر، بحيث نصبح غير قادرين على التمييز بين الراوي والمنتج.

الصنف الثاني: وتمثله فئة النخب سواء أكانت منتمية للأحزاب السياسية أو لمنظمات المجتمع المدني أم كانت مجرد شخصيات مستقلة. ويكون إعلامها البديل عادة أكثر تطورًا وانسجامًا مع مستحدَثات المجتمع الذي يعيشون فيه نظرًا لامتلاكها المستوى التعليمي والموقع الاجتماعي المتميز، ويشكل أعضاء هذه النخب الركيزة الأساس للمجتمع المدني.

الصنف الثالث: يتمثل في فئة النخب الشبابية المهمَّشة، أي أصحاب الشهادات وخريجي الجامعات. وقد عانت هذه الفئة شكلين من

التهميش: تهميش السلطة لها وتهميش المجتمع المدني، وذلك لحرمانها من المواقع الاجتماعية المرموقة داخل السلطة وداخل المجتمع المدني.

- **المشاركة السياسية الإلكترونية**

رافق انخفاض المشاركة السياسية لدى المواطنين من خلال المؤسسات السياسية التقليدية، وعزوف المواطنين عن الانخراط في العمل السياسي الحزبي، البحث عن نوع من المشاركة السياسية تمتاز بأقل قدر من العقبات، فظهرت مواقع التواصل الاجتماعي كنمط جديد من المشاركة السياسية تتيح لمستخدميها إمكانية نشر المعلومة السياسية دون عوائق، مما يساهم في رفع الوعي المشترك بين المواطنين.

وفي إطار نمو الدور الذي باتت تلعبه مواقع التواصل الاجتماعي، والمنظمات الطوعية في استقطابها لاهتمامات الأفراد والمجموعات، وفى التعبير عن آرائهم في الشؤون الخاصة والعامة دون قيود، لم تعد الأحزاب السياسية هي المؤسسات الوحيدة التي تعبر عن الاتجاهات السياسية، وتُقدّم مصالح الأفراد والفئات المختلفة في المجتمع. وجاء التطور التقني واستقصاءات الرأي العام المستمرة حول القضايا السياسية والاجتماعية والثقافية، كبديل عن الخطابات السياسية المعتادة للأحزاب.

ولكن يظل السؤال المطروح هو: هل يمكن اعتبار الشخص الذي يقوم بكتابة تعليق سياسي على حسابه الشخصي ناشطًا سياسيًا؟ وهل يمكن التعامل مع هذا الفعل كنوع من المشاركة السياسية؟

تكمن الإجابة عن هذا التساؤل عن طريق تصنيف الناشطين السياسيين في ثلاثة أنماط:

1. الناشطين سياسيًا في الفضاء الإلكتروني فقط، وهم غير ناشطين خارجه.
2. الناشطين سياسيًا خارج الفضاء الإلكتروني فقط.
3. الناشطين سياسيًا داخل الفضاء الإلكتروني وخارجه.

ويجب عدم الخلط بين هذه الأنماط الثلاثة عند التحليل، لمعرفة مدى تأثير هذه المواقع على عملية صناعة القرار.

ولا بدّ هنا من الإشارة إلى مساهمة مواقع التواصل الاجتماعي في تسهيل الحراك السياسي بين الأفراد، وتعزيز القدرة على اتخاذ فعل جماعي، لأنها تعتبر منبرًا تستخدمه الحركات الاجتماعية المختلفة لنشر أفكارها ودعوة الآخرين إلى اعتناق تلك الأفكار، إضافة إلى دور تلك المواقع في تحفيز الفعل الجماعي إلى جانب المؤسسات السياسية التقليدية.

ويمكن الإشارة أيضًا إلى بروز ممارسة سياسية جديدة تتمثل في رغبة الأفراد والمجموعات تجاوز وساطة جميع البنى السياسية والمدنية

والنقابية والمؤسساتية المنظمة، والتحرك تلقائيًا دون مواجهات مباشرة مع السلطة، بالارتكاز على الثقافة الرقمية كأداة للتأثير والفاعلية والإقناع والتوافق والانخراط الجماعي، فالممارسة السياسية الافتراضية بالنسبة للفرد والمجموعات صارت هي الضامن لاستمرارية الممانعة والتعبئة والتحدي الإيجابي.

لقد رسخت شبكة الإنترنت نفسها كأداة للمشاركة السياسية، يتم تمكين الناس فيها من المساعدة في تشكيل عملية صنع القرار السياسي بالمعنى الحقيقي للديمقراطية المستدامة، من خلال الشبكات الاجتماعية في منتديات المناقشة، أو ببساطة على مواقع المنظمات. ووفقًا لدراسة أجرتها الجمعية الفيدرالية الألمانية لتكنولوجيا المعلومات والاتصالات ووسائل الإعلام الجديدة (BITKOM) عام 2013، يرى معظم المستخدِمين أنّ الإنترنت أداة لتعزيز الديمقراطية، إذ يشارك كلّ مواطن في الحملة الانتخابية عبر الإنترنت، وهناك نسبة أربعة وستين بالمائة من الشباب الذين تتراوح أعمارهم بين 18 و 29 سنة يختارون هذه الوسيلة.

وفي عام 2008، أظهر الرئيس الأمريكي المنتخب باراك أوباما – خلال الفترة الانتقالية إلى رئاسته – ما يدور حوله من كلّ هذا بطريقة مثالية، عندما أتاح العديد من فرص المشاركة الإلكترونية على موقع البوابة change.gov، مثل «منتدى المناقشة ومواطنون»، حيث يمكن لأي

شخص أن ينشر رأيه في أي قضايا سياسية يرغب في معالجتها، أو التعليق على آراء الآخرين. وتم إرسال الآراء والتعليقات حول تلك القضايا مباشرة إلى الرئيس. ولا يزال بإمكان المواطن الأمريكي اليوم طرح الأسئلة والتعبير عن آرائه على موقع البيت الأبيض على الإنترنت.

- **مخاطر المشاركة الإلكترونية: الانقسام الرقمي**

بقدر ما تحفز المشاركة الإلكترونية الحوار، يظل كل من لا يستطيعون الوصول إلى الإنترنت مستبعدين من المناقشة. ولا يقتصر انقطاع الاتصال هذا على الوصول الفني إلى الإنترنت، لأنه حتى لو أصبحت المشاركة الإلكترونية ممارسة قياسية في دول مثل ألمانيا، يجب على الأشخاص التعلم أو التدريب على كيفية استخدام الإنترنت كأداة. وعلاوة على ذلك، يبدو من الصعب أن ينظر الناس إلى فرص المشاركة ويتصرفوا بها بطرق مختلفة تمامًا، وحتى الآن يبدو أن الشباب والمهاجرين وشرائح المجتمع غير المتعلمة يتمتعون بنسب مشاركة أقل بكثير من الآخرين في العملية السياسية.

يلاحظ الباحث الإعلامي البروفيسور جيرهارد فون من جامعة هاينريش هاينه في دوسلدورف أن الفجوة التعليمية تنعكس في هذا الاتجاه، ويبين من خلال تجربته أنّ المتعلمين تعليمًا عاليًا هم أكثر من

يستخدمون الإنترنت في مصلحتهم السياسية، ولا يمكن للرسائل السياسية الوصول إلى الأشخاص الأقل تعليمًا من خلال هذه القناة.

- **الطابع الأيديولوجي لمواقع التواصل الاجتماعي**

يُعَدّ الطابع الأيديولوجي لمواقع التواصل من مُحدِّدات الحروب الإلكترونية التي يشنّها الأفراد أو الجماعات أو الدول لاستهداف مواقع شبكات التواصل الاجتماعي، إذ تكشف هذه الهجمات الطابع الأيديولوجي لهذه الحروب، وتؤكد من جانب آخر الصراع حول المعاني والأفكار والتصورات التي تحملها المضامين الإعلامية لتلك المواقع، فهو صراع أيديولوجي. وبهذا المعنى تكون الشبكات منصات لصراع أيديولوجي فكري أو عقائدي أو مذهبي أو سياسي، أو صراع حول النفوذ والمصالح. وتتحول إلى وسائط حرب أيديولوجية وفكرية بالموازاة مع الحرب التقليدية. ويرسم التدفق المعلوماتي - الذي يشكل بمصادره المختلفة سيلًا منهمرًا باتجاه مستخدمي الشبكات الاجتماعية -طريقة التفكير أو ما يجب أن يفكر فيه المستخدم ويعرف عنه ويشعر به، وهو جوهر مضمون الإعلام المؤدلج.

يُعتَبر دور شبكات التواصل الاجتماعي واستراتيجياتها في تشكيل الرأي العام، من أبنية نظرية إعلامية متعددة ومداخل مختلفة، أساسيًا لتحديد التأثير الذي تُحدِثه الشبكات الاجتماعية في المستخدمين.

وتشمل هذه المداخل نظرية التسويق الاجتماعي التي تتناول كيفية ترويج الأفكار التي تعتنقها النخبة في المجتمع لتصبح ذات قيمة اجتماعية مُعترَف بها. وتقوم وسائل الإعلام وفق هذه النظرية بإثارة وعي المستخدمين عن طريق الحملات الإعلامية التي تستهدف تكثيف المعرفة لتعديل السلوك، بزيادة المعلومات المرسَلة للتأثير على القطاعات المستهدَفة من الجمهور.

وتعتمد أهمية الثورة الاتصالية الكبرى والتكنولوجيا الجديدة لوسائل الإعلام الإلكترونية في ظهور فضاء عام اجتماعي جديد، على أن يكون الرأي العام حرًا في حركة المعلومات وتبادل الأفكار بين المواطنين. وتؤكد نظرية المجال العام أنّ وسائل الإعلام الإلكترونية تخلق حالة من الجدل بين الجمهور، وتُحدِث تأثيرًا في القضايا العامة، وتؤثر في الجهة الحاكمة. ويمكن رؤية المجال العام كمجال حياتنا الاجتماعية الذي يمكن من خلاله تشكيل الرأي العام، إضافة إلى دور مواقع التواصل الاجتماعي في تحقيق الديمقراطية، إذ يُنظَر إلى المجال العام هنا كمحيط سياسي. ويحدث تأثير شبكات التواصل الاجتماعي في الرأي العام من خلال ثلاثة مستويات مترابطة، تتمثل في: المستوى العاطفي، حيث يؤدي تزايد المجموعات عبر الشبكات إلى إعادة صياغة العواطف، والتأثير في الأذواق والاختيارات بناء على النموذج الـمُقدَّم في هذه المجموعات. ثم المستوى المعرفي، وهو مرتبط بالبعد السابق، فقد أصبحت المجموعات

مصدرًا جديدًا من مصادر إنتاج القيم وتلقين المعارف (الأيديولوجيا) وتشكيل الوعي بالقضايا المختلفة. والمستوى الثالث هو البُعد السلوكي الذي يُعَدُّ أعمق هذه المستويات ولاحقًا لها (مكاوي، 2009).

إنّ شبكات التواصل الاجتماعي لا تنشأ في الأصل من فراغ بل تخضع إلى اعتبارات أيديولوجية، فمؤسسو الشبكة سواء كانوا أفرادًا أم جماعات يتبنون أفكارًا معينة، وتنشأ بناء على ذلك أفكار الشبكة (نموذج شبكة الفيس بوك)، وهذا لا يعني أن هناك حالة سكونية في البناء الشبكي، فقد تتغير الوجهات الفكرية لمؤسسي الشبكة تبعًا لتغيير الأيديولوجيا المسيطرة على تفكيرهم، وخصوصًا أنّ الأيديولوجيات ليست حتمية، ولذلك ظهرت مُحدِّدات تبرز الطابع الايديولوجي للشبكات الاجتماعية ومنها (مصطفى، 2014):

- الأيديولوجيا السياسية وما يدور حولها من أحداث، فقد أصبحت هذه الشبكات أشكالًا من المداولة والنقاش حول الشأن العام، وسمحت للنخب السياسية بتجاوز آليات تغييبها في المجال العمومي التقليدي الذي تسيطر عليه الدولة.
- لا تعمل الشبكات الاجتماعية بمعزل عن سياقها أي (المجتمع الافتراضي)، وإذا كانت الفرضية الأساسية للمجتمع الافتراضي منذ نشأته ترتكز على مشاركة الاهتمامات، فإنّ الأفراد أو الجماعات يحتكمون عند دخول الشبكات الاجتماعية إلى

الاهتمامات التي تُعَدّ بدورها محدِّدًا أيديولوجيًا ينطوي على عنصر اختيار يستمد مرجعيته من الأطر الفكرية الحاكمة للمستخدمين.

- أفرزت الشبكات الاجتماعية أشكالًا جديدة من الفعل الجماعي، وخلقت فضاءات بديلة اقتضت جماعات افتراضية، وتكونت حولها مشاغل مشتركة سياسية واجتماعية وفنية ورياضية ومهنية تنطلق من أيديولوجيات متعددة.

إن بروز قادة رأي عام حدد لهم منابرهم الإعلامية وتقنياتهم الخاصة لحشد الجماهير وتعبئة الأفراد، وقد تكون هذه من أهم المحدِّدات الأيديولوجية للشبكات الاجتماعية، وذلك لأنّ قادة الرأي العام في مواقع التواصل يؤثرون في المجتمع، وقد أصبحوا فاعلين وباستطاعتهم أن يغيروا في الحياة الاجتماعية والسياسية. ومع هذا، وفي ظل تحولات العالم السياسية - وخصوصًا الواقع العربي - برز فاعلون جدد من مختلف دول العالم لا يدخرون جهدًا في التسلل إلى المجتمع الشبكي الذي أصبح نظامًا للعلاقات السياسية والاجتماعية والإنسانية والاتصالية ومتحكما فيها أيضًا، إذ يحاول هؤلاء استغلال أية وسيلة أو منصة لتكون وسمًا لهويتهم.

- أثر مواقع التواصل الاجتماعي على علاقة الفرد بالدولة

نادرًا ما يكون النشاط بين الأشخاص بوساطة الإنترنت محايدًا، وغالبًا ما يميل إلى إنتاج تأثيرات اجتماعية متناسقة، حيث لا يمكن ملاحظة ازدواجية في أي مكان آخر في مجال الصراع، فللإنترنت القدرة على تحفيز التماسك القتالي أو تحطيمه.

ومن الناحية الإيجابية، يصور المُنَظِّر في السياسة الخارجية «أودري كورث كرونين» الإنترنت على أنه حشد جماهيري شبكي يؤدي إلى عصر جديد من الصراع. وعلى النقيض من ذلك يرى P.W. Singer و Emerson Brooking، في كتاب (Like War) أنّ وسائل التواصل الاجتماعي على الإنترنت يمكن «تسليحها» لخلق ارتباك في الخصم، مما يؤثر سلبًا على الإرادة والقدرة على القتال. ومع ذلك، تم إيلاء اهتمام أقلّ بكثير للتأثير الموهِن لاستخدام وسائل التواصل الاجتماعي على العلاقات بين المواطنين والدولة القومية، ولا سيما القوات المسلحة، ولذلك فمن المرجَّح أن تتراكم الآثار الاجتماعية والنفسية والعصبية لاستخدام وسائل التواصل الاجتماعي لتقليص المشاركة العسكرية بشكل كبير في الديمقراطيات، مما يحدّ من استخدام القوة العسكرية كأداة للسياسة الخارجية.

يُعَدّ الإنترنت أمرًا مهمًا داخل المجتمع لأنّ هذه الشبكة التي تتعامل معها الأجهزة أصبحت منتشرة بشكل لا يمكن التغافل عنه، فالاتصال بين

الأشخاص عبر الإنترنت أمر سهل وغير مُكلِف، ويولِّد على الفور روابط وعلاقات اجتماعية جديدة، ولذلك تكون الآثار سريعة وواسعة الانتشار.

يمكن القول بأننا نكون جميعًا من خلال وسائل التواصل الاجتماعي مستهلكين ومنتجين وناشرين للمعلومات، فكما يلاحظ عالِم الاجتماع زيغمونت باومان (Zygmunt Bauman): «يأمل الفرد باستخدام هذه المنصات في الارتقاء بالأفعال الخاصة إلى أحداث عامة وسيرة ذاتية في التاريخ»، وإنشاء مجال شخصي يمكن تعميمه في الشبكات اللامركزية كتجربة شخصية.

وينغمس الفرد في وسائل التواصل الاجتماعي، ويظهر في العديد من المجتمعات المتنافسة المتداخلة، حيث يتم إنشاء علاقات قوية من المعاملة بالمثل من خلال الهياكل المحفِّزة مثل «الإعجابات» و«المشاركات» و«المتابعين»، حيث تثير هذه الهياكل الرغبة لدى المستخدم في إنشاء مواد ومعاملات بشكل مستمر. ويشير مؤسس تويتر جاك دورسي في شهادته أمام لجنة الاختيار في مجلس الشيوخ للاستخبارات في 2018 إلى التأثيرات على توليد البيانات، فقد استغرق الأمر ثلاث سنوات بعد أول تغريدة لدورسي في عام 2006 لتصل إلى مليار تغريدة إجمالًا. واليوم، هناك ما يقرب من مائتي مليار تغريدة في السنة لمستخدمي تويتر. ووفقًا لشركة ذكاء الأعمال دومو، استخدم الأمريكيون في تصفح التويتر ما معدله 4,416,720 غيغابايت من البيانات

في الدقيقة في عام 2019. ووجد مركز «بيو للأبحاث» أنّ ستة أشخاص من كل عشرة من مستخدمي Snapchat وInstagram، المنصات الأكثر شعبية بين المواطنين الرقميين، يزورون هذه المواقع يوميًا.

والآن بعد أن تم تمكين حياتنا الاجتماعية بشكل روتيني إلكترونيًا، يتم تنفيذ الإجراءات التي كانت غير مرئية إلى حدّ كبير على المسرح العام بوساطة «الطوائف الإلكترونية المحمولة»، فمن خلال التعبير عن قصص الحياة على هذه المنصات تم إدخال المعنى والغرض في الحياة، وهو الانغماس في هذه الشبكات الاجتماعية، من خلال تعزيزها الدائم للمقارنة والمنافسة، وهو ما يؤدي إلى تآكل التجاذبات الموجودة بين الفرد والدولة القومية بطرق غير مرئية، فالهوية والقيم أصبح من الممكن توفيرها من قبل الشبكة، مما يقلل من أهمية الدولة القومية في حياة الفرد.

إنّ العقد الاجتماعي بين الفرد والدولة الذي يكثف ويوحد القيم مثل الدين والأسرة تحت سلطة سياسية واحدة يتم حجبه بسرعة من خلال وسائل التواصل الاجتماعي، فتملأ هذه المنصات الرغبة الإنسانية في المشاركة والاعتراف بشكل أكثر حدة بالدولة الديمقراطية. أمّا المواطنون الرقميون، وهم الجيل الأول المنغمس في الأجهزة المتصلة بالإنترنت منذ الطفولة، فإنّ هذه المنصات هي بيئاتهم الاجتماعية الأساسية.

وقد تمّ تدريجيًا وبخطوات هيكلية استبدال العلاقات المتينة في المجتمعات المادية بعلاقات رقمية سريعة الزوال، وهذه الروابط لها آثار نفسية عميقة، ففي كتابه «القبيلة»، يقول الصحفي الحربي سيباستيان جونجر: «إنّ القدرة على التنبؤ والأمن في الحياة الأمريكية اليومية أصبح يتطلب منا أن نتكاتف معًا من أجل البقاء، وهو شيء يجعلنا نشعر وكأننا قبيلة».

- **مواقع التواصل الاجتماعي في أيدي التنظيمات الإرهابية**

لا شك في أنّ ظاهرة الإرهاب تحظى باهتمام الشعوب والحكومات في شتى أنحاء العالم لما لها من آثار خطيرة على أمن الدول واستقرارها، بعد أن اتضح أننا أمام ظاهرة إجرامية منظمة تهدف إلى خلق جو عام من الخوف والرعب والتهديد باستخدام العنف ضد الأفراد والممتلكات، مما يعني أنّ هذه الظاهرة الخطيرة تهدف إلى زعزعة استقرار المجتمعات، والتأثير في أوضاعها السياسية، وضرب اقتصاداتها الوطنية، عن طريق قتل الأبرياء وخلق حالة من الفوضى العامة، بهدف تضخيم الأعمال الإرهابية وآثارها التدميرية في المجتمع، بما يتناسب مع القاسم المشترك الذي أمكن التوافق عليه بين تعريفات الإرهاب المختلفة، والذي يرى في الإرهاب استخدامًا غير مشروع للعنف يهدف إلى الترويع العام وتحقيق أهداف سياسية، ما جعل البعض ينظر إلى الإرهاب باعتباره

عنفًا منظمًا موجهًا نحو مجتمع ما أو حتى التهديد بهذا العنف – سواء أكان هذا المجتمع دولة أم مجموعة من الدول أو جماعة سياسية أو عقائدية – على يد جماعات لها طابع تنظيمي تهدف إلى إحداث حالة من الفوضى وتهديد استقرار المجتمع من أجل السيطرة عليه أو تقويض سيطرة أخرى مهيمنة عليه لصالح القائم بعمل العنف في إشارة إلى اعتماد الإرهاب المفرط على العنف المتعمد وعدم التمييز بين المدنيين وغير المدنيين كأهداف شرعية من أجل تحقيق أغراض سياسية (الدعجة، 2008: 3).

وتُعَدّ ممارسة القوة عبر الإنترنت إرهابًا إذا صاحبتها دوافع سياسية، مثل التأثير في القرارات الحكومية أو الرأي العام. ويتم ذلك من خلال ثلاثة أبعاد مهمة، يتمثل أولها في توفير المعلومات عن الأهداف المنشودة لتنفيذ عمليات إرهابية تقليدية، فهو مساعد للإرهاب التقليدي، أو وسيط في عملية التنفيذ، أما البعد الثاني فيُستخدَم فيه الفضاء الإلكتروني للتأثير في المعتقدات، مثل التحريض على بث الكراهية الدينية، وحرب الأفكار، في حين يتم البعد الثالث في صورة رقمية، حيث تقوم الجماعات المتطرفة على اختلاف أشكالها باستغلال مزايا الفضاء الإلكتروني كعنصر حيوي يدعم وتحقيق أهدافها، ومنفذ لوجستي داعم وحاضن لنشاطها الإعلامي في مناطق مختلفة من العالم.

وفي هذا الصدد يمكن القول إنّ الجيل الحالي من مقاتلي التنظيمات الإرهابية، مثل تنظيم القاعدة وداعش، هو جيل مختلف عن الجيل الأول من المقاتلين الذي كان يرتكز في عمليات التجنيد على العلاقات الشخصية والتفاعل وجهًا لوجه بين أشخاص ينشرون خطابًا مُحرِّضًا على العنف، ويستخدمون الأفكار والمبادئ الدينية والقناعات الفكرية لتجنيد الأعضاء. أما الجيل الحالي فهو نتاج «ثقافة الإنترنت»، فمن خلال تويتر – على سبيل المثال – يقوم شباب التنظيم بتداول الأخبار أو المقاطع المُصوَّرة التي تحث على نصرة الدين والجهاد على مواقعهم، وجعلها متاحة لأكبر عدد من المتابعين الذين يقومون بدورهم بإعادة التغريد، لتصل إلى آلاف المتلقين، ليس فقط في العالم العربي، بل في العالم أجمع، وهو ما يفسر تمكن القاعدة وداعش من تجنيد شباب من المسلمين الذين يعيشون في الغرب.

وإمعانًا في خلق أجواء الفوضى والترويع، وإتاحة المجال أمام انتشار الشائعات المغرضة التي تثير خوف الرأي العام، وتؤلبه ضد السلطات المحلية بحجة عجزها عن حماية أمنها، يعمد الإرهابيون إلى التسلح بوسائل الإعلام المختلفة لتسويق أغراضهم وغاياتهم وتوظيفها في تضليل الأجهزة الأمنية واكتساب السيطرة على الرأي العام عن طريق نشر أخبار العمليات الإرهابية التي يقومون بتنفيذها، على اعتبار أنّ الحملات الإعلامية التي تغطي هذه العمليات تساعد على تحقيق واستكمال

أهداف الإرهابيين، الذين يرون في التغطية الإعلامية لجرائمهم معيارًا هامًّا لقياس مدى نجاح فعلهم الإرهابي، لدرجة أنّ بعضهم اعتبر العمل الإرهابي الذي لا ترافقه تغطية إعلامية عملًا فاشلًا، من هنا يأتي استغلال الإرهاب للإعلام لترويج فكره الإرهابي ودعمه من خلال محاولاته المستمرة في البحث عن الدعاية الإعلامية لتسليط الضوء على وجوده وأغراضه.

ويستخدم الإرهابيون مواقع التواصل الاجتماعي نظرًا لما تتيحه لهم من قدرة على التواصل مع الآخرين، وخصوصًا من فئة الشباب عبر العالم لبث أفكارهم بطرق مدروسة بشكل دقيق لإقناع هؤلاء الشباب بذلك الفكر المتطرف، سواء من خلال الدين أم المبادئ التي يروجون لها أو الأفكار المتطرفة التي تتسم بالعنف في منهجها، وتستغل اندفاع وطاقات الشباب ورغبتهم في الوصول إلى الأفضل، وعدم إلمامهم بتلك الأفكار ومعرفتهم لطبيعة هويتها ودورها في تضليلهم واجتذابهم للإيمان بها، ومن ثم جعلهم عناصر فاعلة في تنفيذ عملياتهم الإرهابية كلٌّ في وطنه وهو ما يتيح لهم انتشارًا واسع النطاق في كل العالم بالإضافة لعدم قدرة الأجهزة الأمنية على رصد تلك العناصر التي يتم تجنيدها عبر الإنترنت، حيث لا يتم التعرف عليهم إلا عندما يقومون بارتكاب عملياتهم الإجرامية (حسان، 2017: 1).

تعمــد التنظيمــات الإرهابيــة في اســتهدافها الشخصــيات العامــة والمسؤولين الحكوميين على نوعية المعلومات المنشـورة على شبكات التواصل الاجتماعي، والتي تقـترب إلـى حـد كبيـر مـن نشـر تفاصيل عـن مجريـات الحيـاة اليوميـة لمسـتخدمي هـذه الشـبكات، وهـو مـا أسـهم في إمكانية استخدام هذه المعلومات لأغراض إرهابية، من خلال استهداف الشخصيات العامـة والمسـؤولين في جهـات سـيادية، مـن خـلال رصـد تحركـاتهم، ومتابعـة ذويهـم وعـائلاتهم، وهـو مـا يُعـرّض المسـؤول ومَـن حوله والأمن القومي للبلاد لخطر الاستهداف.

وعلى الرغم من عدم الإعلان حتى الآن عـن ثبـوت استهداف إحـدى المنشـآت المدنيـة أو العسـكرية مـن خـلال متابعـة شـبكات التواصـل الاجتماعي وصفحاتها الخاصة من قبل الإرهابيين، فإنّ ثمة سـوابق دوليـة في هذا الإطار، فهجمات مومباي عام 2008 أُعلِن أنّها قد تمـت مـن خـلال المتابعة والاعتماد على معلومات كانت تنشرها نائب مساعد وزير شؤون الدبلوماسية عن أماكن تواجدها على صفحتها الخاصة على «فيس بـوك»، وقد استفاد منها الإرهابيون في القيام بعملياتهم. وهو أمر يدعو إلى تـوخي الحـذر مـن قبـل العـاملين في الجهـات الحيويـة في الدولـة، ويسـتوجب الحـرص في نشـر الصـور والإعـلان عـن أمـاكن التحـرك والتواجـد بشـكل يسـهل مـن مهمـة الإرهـابيين الـذين اعتمـدوا خـلال الفـترة الأخيـرة علـى

عمليات استهداف الشخصيات العامة، والإعلان عن قائمة اغتيالات تضم مسؤولين وشخصيات عامة (صقر، 2014، 207).

إنّ وجود مُحددِّات مرتبطة بخصوصية مجتمع المعلومات دفع بعض الجماعات المسلحة والتنظيمات الإرهابية إلى أن تجعل من شبكات التواصل عنوان هويتها الإلكترونية، وسعت إلى إنشاء شبكات خاصة، على سبيل المثال (نموذج خلافة بوك) وهو موقع للتواصل الاجتماعي أطلقه أنصار تنظيم الدولة الإسلامية ليكون عنوانًا دالًا على كينونتها، تنشر عبره دعايتها ونسقها الفكري، لكنه أصبح خارج الخدمة بعد يوم واحد من إطلاقه. ولا تكون المنصة أو الوسيلة هنا مجرد حامل للخطاب أو الرسالة الإعلامية المؤدلَجة لهذه الجماعة أو ذاك التنظيم، بل تصبح تلك المنصة هي الوسيلة والرسالة في ذاتها.

وهذا المحتوى الإلكتروني الذي يتم بثه من خلال تلك المواقع يمكن أن يشكل تهديدًا لأمن الدول والأشخاص، وخصوصًا الدردشة الإلكترونية التي يمكن من خلالها أن يتم تبادل المعلومات التي تمس الأمن القومي، وتجنيد الشباب للعمل ضمن الخلايا الإرهابية والتنظيمات المتطرفة التي تعمل لحساب قوى معادية تستهدف أمن الوطن واستقراره، ويتم تجنيد الشباب وإغواؤهم عن طريق المنتديات وصفحات التواصل عبر الفيس بوك وتويتر، وهو ما يشكل تهديدًا كبيرًا للعاملين في الهيئات الحيوية للدولة بشكل خاص لمحاولة استدراجهم أو تجنيدهم، بالفكر المتطرف والدخول إليهم عن طريق الدين والجهاد في

سبيل الله والشهادة والجنة، أو استدراج الأفراد لنشر معلومات خاصة بهم ووظائفهم من خلال الفيس بوك أو تويتر، ثم دراسة جوانب شخصياتهم من خلال ما يقومون بنشره على صفحاتهم الشخصية لتحديد وسيلة لاستدراجهم للوقوع في براثن الإرهابيين، وإقناعهم بالقيام بأعمال إرهابية تضر المجتمع والدولة. ومن أسباب جاذبية مواقع التواصل الاجتماعي للتنظيمات الإرهابية:

1. قدرتها على تحقيق التواصل الاجتماعي مع الآخرين بكل اللغات والثقافات لمختلف شعوب العالم.
2. عدم وجود رقابة على التواصل بين أطراف الاتصال.
3. تميّز الاتصالات بالخصوصية.
4. إقبال الشباب على هذه الوسيلة بشكل كبير.
5. انتشار المواقع الفكرية لرموز الفكر التكفيري وتواصلها بخطاب تحريضي جذاب مع زوارها ومعتنقي هذه الأفكار.
6. يعلم المتطرفون الجدد أنّ رموز الفكر التكفيري لم يُعرَفوا بشكل جماهيري إلا عن طريق المواقع الإلكترونية التي روجت لأفكارهم واستقطبت الأتباع.
7. تشكل المنتديات الحوارية المتطرفة وقود الصراع الفكري للفكر المتطرف مع خصومه، إذ يكاد عدد زوار بعض هذه المواقع يتجاوز ربع مليون زائر في إجازات نهاية الاسبوع.

8. تشكل القوائم البريدية التي يشرف عليها مديرو المواقع الإلكترونية حلقة الوصل بين أقطاب الأفكار المضلِّلة والأتباع الذين ينشرون هذا الفكر في دوائرهم الخاصة، وهو ما يعزز من تأثيرها.

يُلاحَظ أنّ الجماعات الإرهابية بدأت خلال الفترة الأخيرة تستفيد بشكل كبير من قدرة وسائل التواصل الاجتماعي على نشر محتويات مخطط الحرب النفسية ضد أجهزة الدولة، وليس أدل على ذلك من الفيديو الذي نشره تنظيم «أنصار بيت المقدس» الإرهابي لمجزرة كرم القواديس بسيناء في أكتوبر 2014، التي استُشهِد على إثرها 31 من جنود القوات المسلحة المصرية، من خلال تفجير الكمين بواسطة سيارة ملغومة، ثم قيام مسلحين بمهاجمة الجنود الذين نجوا من التفجير وقتلهم، والاستيلاء على كمية كبيرة من الأسلحة والذخائر النوعية التي كانت موجودة في الموقع. والحقيقة أنه لا يُمكن النظر إلى قيام التنظيم بتصوير تلك العملية وغيرها، وبثها على المواقع والصفحات الخاصة به على أنه تصوير لمجرد توثيق للحظة، والتأكيد على أنه من قام بها، ولكنّ هدف التنظيم من خلال إقدامه على هذه الخطوة هو إثارة الذعر والخوف، وخصوصًا أن هذا التنظيم أعلن مبايعته لتنظيم الدولة الإسلامية (داعش) الذي يستخدم نفس الأسلوب (الشوري، 2015، 159).

ويُعتبر «تويتر» إحدى أهم وسائل التواصل الاجتماعي التي تستخدم للتفاعل والتنسيق أثناء العمليات الإرهابية، وتكمن الميزة الأساسية في «تويتر» في أنه يوفر مجتمعات افتراضية متغيرة، تتكون بصورة تلقائية خلال الأحداث الكبرى، وهو ما تستفيد منه تلك الجماعات من خلال متابعة أحدث المعلومات عن أي قضية تظهر في المجال العام. ولعلّ المثال البارز على ذلك هو الهجوم الإرهابي في مومباي في 26 نوفمبر 2008 الذي راح ضحيته نحو 164 شخصًا وجُرِح أكثر من 300 شخص. وقد كشفت التحقيقات أنّ جماعة «عسكر طيبة» الباكستانية كانت تقوم بالتنسيق مع منفذي الهجوم من باكستان، وإبلاغهم بالتطورات التي تحدث كافة من خلال الاعتماد على أحدث الأخبار المنشورة على تويتر، مثل تحركات وحدات مكافحة الإرهاب الهندية وتمركزها.

تستخدم المنظمات الإرهابية مواقع التواصل الاجتماعي كأداة لتحديد أهدافها والتعرف عليها ومراقبة تحركاتها، وخصوصًا في إطار عمليات الاغتيالات في الدول المستهدفة، وذلك إمّا بمراقبة مَن يمتلك حسابات على تلك المواقع، أو مراقبة دائرة أصدقائهم ومعارفهم للوصول إليهم، وجمع البيانات اللازمة عن تحركاتهم، وتوفير الوقت والجهد اللازمين للقيام بذلك على أرض الواقع، ولضمان سرية المراقبة أيضًا. ومن ثمَّ، تُعدّ وسائل التواصل الاجتماعي مهمة لتلك الجماعات في إطار ما أسماه بعضهم «شبكات الكوادر» التي تعمل على التواصل بين كوادر التنظيم المسلح كأداة عابرة لقيود المكان، وذلك من أجل مهام منها التدريب على تكوين خلايا تنظيمية، واستقطاب مزيد من الكوادر

وتدريبهم على استخدام الأسلحة، والتنسيق للعمليات المسلحة وتوقيتها، والتدريب على صنع القنابل البدائية وغيرها.

وعلى صعيد آخر، تستخدم مؤسسات الدراسات والأبحاث الدولية مواقع التواصل الاجتماعي في جمع المعلومات وتحليل عمل المنظمات الإرهابية ومناصريها، من خلال استعمال برامج متخصصة في هذا المجال. فمن خلال موقع التواصل الاجتماعي (تويتر)، تمكن معهد أبحاث (RAND) للأمن القومي من استحداث قاعدة بيانات كبيرة تميز بين مناصري الدولة الإسلامية في العراق والشام، فعلى الرغم من أنّ الدولة الإسلامية في العراق وسورية (ISIS) طلبت من أتباعها ان يشيروا إليها باستخدام تسمية (الدولة الإسلامية)، يستخدم من يذمونها التسمية المختصرة (داعش).

وباستخدام عينة من بيانات تويتر تغطي فترة عشرة أشهر، استخدمت المؤسسة (كما هو مشار إليه في الجدول 1) التحليل اللغوي في سبيل دراسة المحتوى والمواضيع الرئيسية لدى المستخدمين الذين يستعملون عبارة (داعش) بمقابل أولئك الذين يستعملون عبارة (الدولة الإسلامية) في تغريداتهم، فتم الوصول إلى نتيجة مفادها أنّ المحتوى لدى مستخدمي عبارة (داعش) بكثرة شديد الانتقاد للدولة الإسلامية في العراق وسورية، فالمستخدمون استعملوا مصطلحات مثل داعش الإرهابية، والخوارج، ومقاتلي داعش، وكلاب النار، وكلاب البغدادي، أمّا مستخدمو عبارة (الدولة الإسلامية) فاستعملوا مصطلحات متوهجة مثل مجاهدي التوحيد، وجنود الخلافة، وأسود الدولة الإسلامية. كما ستظهر في

الجدول التالي الكلمات المستخدمة في التحليل اللغوي الذي استخدمه معهد أبحاث RAND للأمن القومي، باستخدام عينة من بيانات تويتر تغطي فترة عشرة أشهر:

المحتوى	مستخدمو مصطلح الدولة الإسلامية	مستخدمو مصطلح داعش
أعضاء تنظيم الدولة الإسلامية في العراق والشام	الموحدون، المجاهدون، جنود الخلافة، أسود الدولة الإسلامية، الاستشهادي.	داعش الإرهابية، خوارج داعش، خوارج العصر، كلاب النار، كلاب البغدادي
تعابير الدولة الإسلامية في العراق وسورية	في ظل الخلافة، أيها الأنصار، أنصار الدولة الإسلامية، أخوة الأنصار، جعله الله من المقبولين، باقية.	جرائم داعش، مقاتلة داعش، مواجهة داعش، ضرب داعش.
دلالات الهاشتاق المتعلقة بالدولة الإسلامية في العراق وسورية	#باقية و تتمدد #الحملة العالمية لدعم الدولة الإسلامية #الحملة الإعلامية لدعم الدولة الإسلامية	#تنظيم_داعش_الإرهابي #داعش_لا_تهاجم_إيران #داعش_تحرق_الطيار_الأردني #داعش_تستعبد_المسلمين

الجدول 1: تحليل مؤسسة RAND، بيانات تويتر منذ تموز 2014 وحتى أيار 2015.

• الحملات الإلكترونية

تُعدّ الحملات الإلكترونية عملًا فرديًا أو شبه فردي، يتحول إلى عمل جماعي «تطوعي» منظَّم يستهدف إحداث التغيير الاجتماعي والثقافي والسياسي داخل المجتمع، عن طريق استخدام الفضاء الإلكتروني كوسيط لحجم التفاعلات أو المزج بينه وبين فاعليات على أرض الواقع. وقد تكون الحملة مجرد رد فعل سرعان ما ينتهي، وقد تتحول الحملة إلى حركة عن طريق قدرتها على الاستمرار وما ترتبط به من قضية ذات أبعاد مختلفة، وكذلك حجم التأييد من جانب المجتمع ومؤسساته المعنية. وتتركز أنواع الحملات الإلكترونية حول حملة يتم شنّها من الفضاء الإلكتروني، وتنتقل إلى التأثير على أرض الواقع، وحملة أخرى تنتقل من أرض الواقع – سواء كانت في شكل أحداث أو وقائع – إلى الانتشار عبر الفضاء الإلكتروني، وهناك نوع ثالث يتم فيه شنّ الحملة داخل الفضاء الإلكتروني بين مستخدميه فقط. ويمكن القول إنّ الحملات الإلكترونية التي تم شنّها تراوحت ما بين الاهتمام بالشأن المحلي والاهتمام بقضايا دولية، وذلك من حيث درجة الاهتمام، أمّا من ناحية الاستمرارية فهناك حملات تميزت بأنها كانت رد فعل وقتي، وهناك حملات تطورت من مجرد رد الفعل إلى تطوير طريقة عملها وإطالة عمرها (عبد الصادق، 2013: 1).

وأدى ذلك إلى تطوير أساليب العمل الاجتماعي في إطار تحول الإنترنت إلى وسيلة إعلام دولية، مع اندماج جميع أنواع الإعلام التقليدية مثل الإعلام المقروء والمسموع والمرئي داخل الإنترنت.

- **أهداف الحملات الإلكترونية**

لقد أصبح الإنترنت أقرب إلى برلمان عالمي يستطيع كلّ فرد أن يُعبّر من خلاله عن رأيه وفكره، ويشارك في صنع القرارات وعملية اتخاذها، كما يستطيع أن يعترض، وهذا ما يُعدّ من أسس الديموقراطية. وقد تم تشكيل مجموعات افتراضية شبيهة بالأحزاب السياسية، تساهم كجماعة ضغط إلكتروني، وتؤثر في القرارات السياسية للحكومات، وفي عملية صنع قرارات السياسة العامة. وأصبح هناك تواصل وتفاعل حيّ بين القادة والمحكومين والرؤساء عبر الاتصال المباشر عن طريق مواقعهم على الإنترنت، كما صارت شبكة الإنترنت ناقلًا لحركة التفاعلات السياسية السلمية أو الصراعية، بما يساعد في عملية صنع القرار في دوائر السياسية الخارجية في العديد من دول العالم ، وخصوصًا مع تغلب الإنترنت على وسائل الإعلام التقليدية كمنافس لها، وقدرته على تخطي الحدود التقليدية، وانتهاك سيادة الدولة الإقليمية بمفهومها التقليدي، وكذلك أصبح مشجعًا للتحول السياسي داخل النظم الاستبدادية، وأصبحت شبكة الإنترنت مؤسسة للتنشئة السياسية ونشر الثقافة السياسية

بما يؤثر على الحراك السياسي والاجتماعي داخل كلّ مجتمع وعلى مستوى العالم كلّه، وأدى إلى تطوير أساليب العمل الاجتماعي في إطار تحول الإنترنت إلى وسيلة إعلام دولية، مع اندماج كلٍّ من أنواع الإعلام التقليدية مثل الإعلام المقروء والمسموع والمرئي داخل الإنترنت. وتهدف الحملات الإلكترونية إلى (عبد الصادق، 2013: 3):

1. التعبير عن رأي أو موقف لا يمكن التعبير عنه في الواقع.
2. التأثير في الرأي العام وأفكار الناس وآرائهم في قضية معينة.
3. تحريك الطاقات والقدرات الشعبية على الإنترنت واستغلالها لأهداف محددة.
4. إيصال الرأي أو الموقف إلى جهات محايدة (أو حتى معادية) لا يمكن الوصول إليها من خلال الواقع، ولا يتم الوصول إليها إلا بهذه الأساليب.

وقد ظهر العديد من صور وأشكال الاحتجاج وشنّ الحملات عبر الفضاء الإلكتروني ومنها:

1. جمع التوقيعات الإلكترونية للمطالبة بتغيير سياسات أو قرارات أو إزالة صور تُعدّ مسيئة أخلاقيًا أو دينيًا.
2. الدخول إلى غرف الدردشة والمنتديات في الإنترنت للقيام بحوارات، وتكوين رأي مناصر أو مناهض لقضية من القضايا، وإنشاء التحالفات السياسية في الإنترنت.

3. نشر أفكار الإضرابات أو الاعتصامات بين أكبر عدد من مستخدمي الإنترنت عن طريق المجموعات البريدية ورسائل المحمول.
4. مهاجمة المواقع الحكومية الإلكترونية أو مواقع الخصوم والقرصنة وسرقة المعلومات ونشر الفيروسات وغيرها.
5. إرسال كم كبير من الرسائل الاحتجاجية إلى كافة الأطراف المعنية بصورة ضاغطة ومزعجة عن طريق البريد الإلكتروني.
6. إنشاء مواقع إنترنت لنشر الأفكار والرؤى الخاصة بالموقف الاحتجاجي، للحصول على تأييد الرأي العام، وتجنيد الموالين والداعمين لفكرة الاحتجاج من جماعات المصالح المختلفة.
7. تأسيس مجموعات على مواقع الشبكات الاجتماعية وجذب أعضاء إليها كمواقع (الفيس بوك) و(تويتر)، وغيرها لخلق شبكة من الاتصال والتواصل بين المجموعة وخارجها.

- **خصائص الحملة الإلكترونية الناجحة**

تنطلق الحملة الإلكترونية عبر أرضية تتكون من عمل الفرق والمسؤولين ونقطة تواصل وتشاور فيما بينهم لتنفيذ مهام الحملة، بالإضافة إلى خلق شبكة من المؤيدين لتلك الحملة بين مستخدمي الإنترنت، أو تحقيق التفاعل مع غيرهم من الجمهور. ويكون هدف الحملة استهداف الشباب على اعتبار أنهم الفئة الأكثر التصاقًا باستخدام

تكنولوجيا الاتصال والمعلومات، والأكثر قابلية للنشاط والحركة، وخصوصًا بين طلبة الجامعات. ولا ضير من جذب بعض رموز المجتمع أو مشاهيره إلى الحملة بما يحقق الانتشار. ويتم إطلاق الحملة عبر موقع إنترنت أو منتدى حواري أو مجموعة نقاش خاصة، أو عن طريق توزيع الملصقات والشعار الخاص بالحملة وأهدافها. وبالنظر إلى طبيعة الحملة غير الربحية فإنّها تعتمد على الجهد التطوعي من جانب مؤيدي الحملة ومناصريها. ويمكن تحديد عناصر الحملة الإلكترونية الناجحة في النقاط التالية (رحومة، 2007: 90):

1. لا بدّ من تحديد أهداف الحملة وإطارها الزمني، كي تظهر النتائج بشكل جيد، ولا تضيع الجهود والأوقات سدى.
2. توزيع المهام بشكل دقيق ومحدد بين جميع الفرق والمسؤولين.
3. الفرق الفني أو فريق الجرافيكس والتصاميم من أهم عوامل النجاح، فمن دونه لا يوجد تعبير حقيقي عن الحملة يمكن عرضه للآخرين، وتحويل الكلمات إلى رسوم وتصاميم معبرة هو سرّ نجاح الحملات.
4. الاستعانة بالمنتديات والقوائم البريدية من أجل نشر موضوع الحملة وفكرتها وأنشطتها وبياناتها.
5. استخدام بريد إلكتروني خاص وموحَّد للحملة من أجل التواصل من خلاله.

6. تكوين مجموعة بريدية خاصة بالحملة من أجل تجميع العناوين البريدية ومراسلتها لاحقًا إذا استجد جديد في الحملة، وهذا الأمر ينجح مع الحملات ذات المدى الزمني الطويل.
7. التواصل مع جهات إعلامية معروفة من أجل إبراز الحملة إعلاميًا وإشهارها.
8. ترجمة الحملة إلى لغات أخرى حسب نوع الحملة وطبيعتها والجهات الموجهة إليهم.
9. إعداد بنرات وتصاميم دعائية تناسب جميع مجالات الإنترنت، مثل المواقع والمنتديات والمدونات، بحيث تكون هذه التصاميم بأشكال وأحجام متنوعة.

- **أنواع الحملات الإلكترونية**

كان للحملات الإلكترونية التي يقف وراءها ناشطون من خلال شبكة الإنترنت والإعلام الجديد بصفة عامة دور في بروز قضايا جديدة تعبر عن مطالب ذات طبيعة فئوية، حيث ظهرت ثلاثة أنواع من الحملات التي ارتبطت بالتطوع أو الحصول على الدعم أو الحشد أو تنظيم فاعليات، ومن هذه الأنواع نوع من الحملات ارتبط بالانتقال من حدث واقعي إلى التفاعل عبر الفضاء الإلكتروني معه، من خلال تكوين التجمعات والروابط الشبكية في شكل مجموعات الفيس بوك أو في المجموعات البريدية أو غيرها.

وهناك نوع آخر من الحملات ظهر كفكرة داخل أحد التجمعات الإلكترونية، ليتم التفاعل معها وانتقالها بين مختلف مستخدمي المواقع الاجتماعية والإنترنت بصفة عامة. وهناك النوع الثالث الذي يفترض أن تكون الحملات الإلكترونية مواكبة لحادث تفاعلي على أرض الواقع، وتلك الحملات يرتبط معظمها بنسق القيم داخل المجتمع. وهذا النوع يساهم على المدى الطويل في تغيير القيم وخلق نسق قيم جديد، رغم أنه قد لا يكون ناجحًا تمامًا وسريعًا، أمّا النوع الرابع من تلك الحملات فهو ذو الطبيعة التوعوية (طه، 2007: 45) (بتصرف).

وتقوم تلك الحملات في مجملها على دعم التنمية الاجتماعية والسياسية والاقتصادية والثقافية، بالإضافة إلى المساهمة في دعم الحكم الرشيد والمحاسبة، وقد تأتي في شكل احتجاج ضد بعض ممارسات أجهزة الدولة، أو احتجاج على أوضاع اجتماعية واقتصادية قائمة، أو احتجاج على قيم المجتمع التي قد يتم النظر إليها على نحو سلبي.

ومن ثم فإنّ التجمعات الإلكترونية التي تُعبّر عن نفسها برد فعل إيجابي من خلال قيامها بشنّ حملات من أجل التأثير في الرأي العام، تأتي لكي تُشبِع حاجة اجتماعية إلى التعارف والتواصل، وتحقيق نوع من الاتصال المباشر والالتصاق بقضايا الشارع. وهذا الاهتمام لا يفرق على أسس سياسية، أو من حيث السن، أو الجنس، أو الدين، وهذا ما يجعل المجتمع يتسع باتساع دائرة الاهتمام بالقضية محلّ الاهتمام، وتحمل

تلك القضية بذلك نوعًا من المصداقية، حيث إنّ أغلب المشاركين لا ينتمون إلى أحزاب سياسية، ولا يتلقون تمويلًا خارجيًا، بل يقومون بعمل طوعي لخدمة المجتمع الذي يعيشون فيه. ويمكن استغلال ما تعبر عنه تلك الحملات من قدرات شبابية في خدمة المجتمع عن طريق تعزيز علاقتهم بأجهزة الدولة بدلًا من تجاهلهم (رحومة، 2007: 100).

وتلعب الحملات الإلكترونية دورًا كبيرًا في التغيير داخل المجتمع، ويتمثل هذا الدور في النقاط التالية:

1. إنّ الحملات الإلكترونية لا ينبغي أن تقاس بمدى نجاحها أو عدد الموقعين أو المشاركين فيها، ولكن بقدرتها على توصيل الاحتجاج إلى المسؤولين، والتعبير عن الجماهير وحقوقها وحرياتها المنتقَصة أو المعتدى عليها.
2. إنّ الرد الحقيقي على الاحتجاجات يجب أن يأتي على شكل مواجهة بأفكار مضادة في ظل حرية التعبير والرأي بدلًا من استخدام الترهيب والعنف.
3. إنّ الاحتجاجات بطبيعتها تأتي تعبيرًا عن واقع اجتماعي مأزوم ومشكلات اقتصادية.
4. إنّ الاحتجاج الإلكتروني يعبر عن ظهور قوى جديدة فاعلة في الحياة السياسية، يمكن الاستفادة منها بعيدًا عن اتهامها بنشر الشائعات أو الفوضى، وذلك لاعتمادها على آليات عمل مختلفة تشكل لها مصادر

قوة جديدة، وتصوغ دورها المستمر في طرق التأثير وتعبئة الرأي العام.

5. إنّ الحملات الإلكترونية والفاعلين فيها تعبير عن واقعهم الاجتماعي الذي يعيشون فيه، ونتيجة لما آلت إليه الثورة التكنولوجية والاتصالية، وهي إضافة جديدة لنشاط الحركات الاجتماعية وما طرأ عليها من تغير في طبيعتها، إضافة إلى أنّ معظم الناشطين في هذه الحملات ينتمون إلى الفئة العمرية للشباب، وهم يعانون من مشكلات ويملكون طموحات مشروعة.

6. يمتلك الفاعلون في الحملات الإلكترونية القدرة على مخاطبة الرأي العام، وصوغ أهدافه، والتلاحم مع مشكلاته بدرجة أكبر وأسرع من المؤسسات التقليدية، وأصبحت تلك الحملات تعبيرًا في الوقت ذاته عن مفارقة هامة مؤداها تزايد دور أدوات الرأي والتعبير عبر الإنترنت مع حالة الحراك الاجتماعي والسياسي.

7. تعبر الحملات الإلكترونية عن دور الإعلام الجديد والاتصالات في دفع عملية التنمية الشاملة التي قد تتم عن طريق التغيير السلوكي والاجتماعي، وهو ما يتطلب استراتيجيات مختلفة ومجموعة فريدة من المهارات، والقنوات الجماعية ووسائط الإعلام والطرق القائمة على المشاركة، وخصوصًا مع دور الفرد المركزي في دعم استراتيجيات تغيير السلوك.

وتختلف الحملات في درجة ثقافة أعضائها وشبكة علاقاتهم وطبيعة هؤلاء الأعضاء، وكذلك في درجة علاقاتهم بمؤسسات الدولة المعنية، فقد كانت الحملات التي تعتمد على استقطاب شخصيات عامة هي الأقدر على التأثير والانتشار، بالإضافة إلى أهمية تفاعل الصحافة والإعلام ورجال الفن مع نشطاء الإنترنت في حملاتهم كي تنتقل هذه الاحتجاجات من المستوى الإلكتروني إلى المستوي الشعبي، وتصل إلى رجل الشارع وتُحدِث أكبر الأثر (طه، 2007: 49).

وتحاول الحملات باستمرار جذب أعضاء جدد إليها من أجل الحصول على جهدهم التطوعي، وكذلك الحصول على دعم الصحافة ووسائل الإعلام الأخرى للمساهمة في نشر المعلومات عن الحملة ومَن يقودها أو ساهم في إطلاقها، وكذلك أبرز ناشطيها بالإضافة إلى نشر الثقافة والوعي بأهمية الحملة (زريقات، 2008: 6).

وعلى الرغم من وجود مثل ذلك الاختلاف في طبيعة الحملات أو في أهدافها أو أعضائها، هناك قدر من التشابه قد يجمع القائمين على تلك الحملات، حيث إنّ هؤلاء لديهم هدف مشترك ومصلحة واهتمام، ويدخل القائمون على هذه الحملات وناشطوها في سجال فكري وتواصل مستمر مع الأعضاء من أجل تطوير الحملة، أو من خلال التفاعل مع بعض الجهات المعارضة أو غير المقتنِعة بالفكرة من أجل التأثير عليهم، أو كذلك من خلال الاتصال بوسائل الإعلام لنشر الوعي عن أهداف الحملة، كما يهدف القائمون على هذه الحملات إلى

الحصول على دعم الجهات الحكومية المختصة أو ذات الصلة بموضوع الحملة (رحومة، 2007: 102).

وأخيرًا فإنّ هناك الكثير من الأساليب التي تعتمدها القوة الناعمة، وهي أكثر خطورة من القوى الصلبة لأنّ الثانية تنشط في المواجهات المباشرة فقط، أمّا الأولى فتنشط في جميع الأوقات. ومن أهم وسائلها: الرسائل الإلكترونية عبر الإنترنت ومواقع التواصل الاجتماعي، والمعارك الكلامية في قنوات البث الفضائي وما يشكله من غزو ثقافي وإلكتروني، والاكتساح الإعلامي بما يسببه من إشاعة لثقافة العنف في المجتمعات من خلال الحملات الإلكترونية التي توظفها الدول أو الأفراد للتعبير عن العديد من القضايا السياسية والاقتصادية والثقافية وغيرها...

الفصل الخامس

أثر حرب الفضاء الإلكتروني
على طبيعة العلاقات الدولية

يتسـم الفضـاء الإلكـتروني بالانتشـار الفـائق والسـيولة، وقوامـه شـبكات الإنترنت، ومئات الملايين من الأجهزة التي تربطها بالمؤسسات والشركات التي تقوم على هذه الشبكة وترتبط بها، والخبرات التي يفرزها. وقد خلق هـذا الفضـاء واقعًـا إنسـانيًا جديـدًا، يمثـل تحـديًا للنظريـة المعاصـرة في العلاقـات الدوليـة، وكـذلك علـى مسـتوى السياسـات والممارسـات. وتمثلـت هـذه التحـديات في عناصـر الوقـت وقـدرة التكنولوجيـا علـى الاخـتراق والارتبـاط والتشبيك.

ومـن هنـا أصـبحت القـوة الإلكترونيـة حقيقـة أساسـية في العـالم بكـلّ مظاهرهـا المتنوعـة، مـا أدى إلـى دعـم ومسـاندة العمليـات الحربيـة والقـوة الاقتصادية والسياسية، وتعزيز دور ثورة المعلومات والمعرفة في تحديد آفاق النمـو أمـام مختلـف البلـدان، يضـاف إلـى ذلـك العمـل علـى توزيـع المـوارد الاقتصـادية ومسـتويات النمـو الاقتصـادي، وأنمـاط التفاعـل بـين القـوى الاقتصـادية الدوليـة، والتـأثير علـى القـوة السياسـية بالتـأثير في عمليـات صـنع القرار في النظـام الـدولي. وقـد لعـب الفضـاء الإلكـتروني بكـلّ مـا يحملـه مـن أدوات ووسائل تقنية حديثة دورًا كبيرًا في طبيعة العلاقات الدولية.

وسيتم التركيز في المبحثين الأول والثاني مـن هـذا الفصـل علـى السـلبيات والإيجابيـات التـي أحـدثها الفضـاء الإلكـتروني في طبيعـة العلاقـات الدوليـة، ومـن ثـم سيتناول المبحـث الثالـث أنمـاط الصـراع الإلكـتروني وخصائصـه، وسيتم في المبحث الرابع مناقشة أهـم التـأثيرات والانعكاسـات الحاصـلة في الشرق الأوسط نتيجة تطور حرب الفضاء الإلكتروني.

• النظرية الواقعية وعلاقتها بالصراع الإلكتروني

تم تعريف القوة السيبرانية على أنها «القدرة على الحصول على النتائج المفضلة من خلال استخدام موارد المعلومات المترابطة إلكترونيًا للمجال السيبراني»، وقد أصبحت قدرتها على تغيير العلاقات الدولية موضوعًا لنقاش بارز، على الرغم من عدم وجود نظرية حول القوة السيبرانية في الأدبيات الواقعية.

تقدم الواقعية إطارًا للتفكير في توزيع السلطة بين الجهات الفاعلة وكيفية ارتباط ذلك بالصراع. ويبدو أن الواقعية - كنظرية معنية في الغالب بقضايا الأمن القومي والسلطة - هي منظور العلاقات الدولية الغريزية لفهم الصراع السيبراني. وتبقى الواقعية إطارًا مناسبًا لتحديد القضايا المهمة المتعلقة بالأمن في المجال السيبراني، ويمكن أن تقدم في بعض الأحيان رؤى مفيدة حول بعض الخصائص الدائمة للعلاقات الدولية. ومع ذلك، غالبًا ما تكون النظريات الواقعية حول الصراع قاصرة بشكل كبير في تفسير الديناميكيات الفريدة للصراع السيبراني.

يشبه المجال السيبراني من نواحٍ عديدة، العالم الواقعي بطبيعته الفوضوية ونقص الحوكمة المؤسسية، حيث تخشى الدول بعضُها بعضًا، وتطور قدراتها في الاستجابة، ومع ذلك من غير الواضح ما إذا كانت سباقات التسلح السيبراني قابلة للتصاعد إلى صراع سيبراني. وتثير الواقعية أيضًا أسئلة مثيرة للاهتمام حول القوة السيبرانية، وحول من يمتلكها، وكيف ترتبط بالاستقرار الدولي، من حيث ما إذا كانت هذه

القوة ستغير ديناميكيات القوة التقليدية. وتشير الأدلة إلى أن الأمر ليس كذلك، فقد تم تقييد الاتجاه الذي رأيناه حتى الآن من الحرب السيبرانية الكاملة لصالح أشكال أقل تدميرًا من التفاعلات السيبرانية.

ولعلّ التوازن بين الدفاع والهجوم هو أوضح مثال على استخدام نظرية واقعية لشرح المجال السيبراني، لكنه يبدو غير دقيق تجريبيًا في افتراضاته حول المجال السيبراني وتنبؤاته حول الصراع السيبراني، حيث تشير حالات الصراع السيبراني في العالم الواقعي إلى أن الجريمة ليست سهلة كما يُفترَض في كثير من الأحيان، وحقيقة أننا لم نرَ الكثير من حالات الصراع السيبراني تشير إلى أنّ النظرية في غير محلها. وعلاوة على ذلك، فإنّ استجلاب الحكم على فكرة الردع من الحقبة النووية هو حكم خاطئ وغير منطقي، ولا معنى له في سياق حقيقة الأسلحة السيبرانية.

إنّ الحكمة، وهي أساس للواقعية الكلاسيكية، قد تقدم النظرية الأكثر قابلية للتطبيق، وكما يلاحظ مكيافيلي، يجب على الأمير «أن يسير باعتدال وبحكمة وإنسانية، كي لا تجعله الثقة الزائدة غير حكيم». ونظرًا للشكوك المحيطة باستخدام التكنولوجيا السيبرانية كسلاح هجومي، يجب على الدول المضي بحذر في المجال السيبراني، والتركيز على إنشاء دفاعات مرنة، ففي الواقع، ظلت العديد من الدول حتى الآن حكيمة إلى حد ما في سلوكها في الفضاء الإلكتروني من خلال امتناعها عن الحرب السيبرانية الصريحة، وهذه نتيجة سيجدها المنظرون الواقعيون جذابة، وسيرون فيها مجالًا لمزيد من التفصيل النظري.

ولهذا كلّه لا بدّ من تطوير نظريات جديدة قائمة على الملاحظة التجريبية أو المنطق الاستنباطي للمجال السيبراني، بدلًا من الرجوع تلقائيًا إلى النظريات الواقعية التي تم تطويرها لشرح الأشكال الحركية للحرب. ويمكننا من خلال إجراء المزيد من الأبحاث التجريبية، الحصول على فهم أكثر دقة للقضايا الرئيسية، مثل تأثير سباقات التسلح السيبراني على العلاقات بين الدول، وتوزيع القدرات السيبرانية بين الجهات الفاعلة الحكومية وغير الحكومية، وأسباب ضبط النفس على الرغم من المنافسة الأمنية الشديدة ووجود تصورات لميزة هجومية، ويمكن أن تساعدنا الإجابات الأكثر دقة عن هذه الأسئلة في صياغة توجيه أفضل لسياسات الحكومات.

• الفرص التي يمنحها الفضاء الإلكتروني لتحديد أنماط العلاقات الدولية

ترتبط القوة الإلكترونية بامتلاك المعرفة التكنولوجية والقدرة على استخدامها، وهي تعني القدرة على استخدام الفضاء الإلكتروني في خلق مميزات، والتأثير في الأحداث التي تجري عبر الشبكات التشغيلية وعبر أشكال وأدوات القوة المختلفة، سواء كانت دبلوماسية أم اقتصادية أم عسكرية أو معلوماتية. وقد حدد جوزيف ناي ثلاثة أنواع من الفاعلين الذين يمتلكون القوة الإلكترونية، يتمثل النوع الأول في الدولة، والنوع

الثاني في الفاعلين من غير الدول، والنوع الثالث في الأفراد. وهناك موارد لاستخدام القوة الافتراضية كالاستخدام الصلب والاستخدام الناعم.

وقد مثّل الفضاء الإلكتروني تحديًا للافتراضات التقليدية من قبيل طبيعة دور الفاعلين في العلاقات الدولية، والتأثير في حالة العلوم الاجتماعية بشكل عام، ومدى الاستفادة من الوسائل والأدوات التحليلية في عملية دفع العلاقات الدولية إلى الأمام، ومدى توظيف التطبيقات الإلكترونية في تطوير عملية النقاش والتحليل والتنبؤ حول العلاقات الدولية، واختيار الفروض والتقنيات التي من شأنها أن تكون ذات فائدة لجميع الأطراف الفاعلين في العلاقات الدولية (عبد الصادق، 2012: 125).

إنّ تطور استخدام الفضاء الإلكتروني بكافة إمكاناته، من خلال تنويع وحسن استخدام وسائل ثورة المعلومات في وقتنا الحاضر، يشكل ركنًا مهمًا ومؤثرًا في قدرة الفاعلين من دول وأفراد ومنظمات دولية وشركات متعددة الجنسيات، وإمكاناتهم التي يستخدمونها، والتي تمكنهم من تمرير أو قبول مشاريعهم السياسية التي قد تتطابق مع الفاعلين الآخرين، مع ضرورة فحص وتدقيق أدواتهم المستخدمة، مع ما يحيط بتلك القدرة من مناخ سياسي دولي ملائم، وهذا يستلزم وجود قيادات خلاقة قادرة على صنع السياسات وليس تنفيذها فقط، فوقائع الثورة العلمية التقنية وثورة الاتصالات والمواصلات وتكنولوجيا المعلومات والطفرة الرقمية «الديجيتال»، لها أكثر من تأثير في طبيعة ومسار العلاقات الدولية.

يدور الفضاء الإلكتروني في محاولة إحداث التحوّل والتغيير في السياسة والاقتصاد والاجتماع داخل النظام الدولي، ويعمل على تعزيز الانفتاح السياسي، والتحوّل الديموقراطي، مع ظهور ما يعرف بالديموقراطية الرقمية (Digital Democracy). كما يظهر الدور الإيجابي للفضاء الإلكتروني في العمل على تخفيف حدّة الصراعات عبر ما يطلق عليه (الدبلوماسية الإلكترونية E- Diplomacy) التي تُعنى بنشر مبادرات السلام، وتعزيز الحوار والتعاون بين دول العالم، والانفتاح العالمي على الثقافات المختلفة. وكذلك عمل الفضاء الإلكتروني على زيادة الوعي العالمي بالخسائر الناجمة عن الصراعات وأثرها على المجتمع الدولي، وتكوين رأي عام دولي يدافع عن خيار السلام لا الحرب، عبر الدبلوماسية الافتراضية (Virtual Diplomacy) وتعزيز الدبلوماسية الشعبية القادرة على التأثير في الرأي العام العالمي.

وقد قرَّب الفضاء الإلكتروني المسافات وتداخل في الأنماط الحياتية التي يعيشها المجتمع الدولي، إزاء ما يقدمه من خدمة سهلة ورخيصة للمتداولين، دون أن ننسى أنّ حاجات الستار والتخندق والانفرادية لم تعد ممكنة في هذا العصر العولمي بحكم تداخل الحاجات الإنسانية بعضها ببعض، حيث أدرك العالم أهمية الاتصالات وتكنولوجيا المعلومات. وتتميز السنوات الأخيرة بالتطور السريع في هذه المجالات، حتى أصبحت مقياسًا لتقدم الأمم والمجتمعات في كافة أرجاء العالم، الأمر الذي دفع الكثير من الدول لوضع خطط وبرامج استراتيجية لتطوير

واقع الاتصالات والتقنيات الحديثة، بالاعتماد على الكفاءات المحلية وخبرات الدول المتقدمة للحاق بركب العالم المتطور (كاريللو، 2011: 172).

وقد أصبح الفاعلون من غير الدول يؤدون دورًا مؤثرًا في سياسات الدول الأمنية، الداخلية والخارجية، وهذا متأتٍ من الفيض التقني المتطور للعلوم وما قدمته من تسهيلات في التشارك والتفاعل في رفد وتعزيز الإطار الاستراتيجي لبلدانهم، الأمر الذي يستوجب فهمًا أعمق لسلوك الجماعات والفاعلين من غير الدول، وعلاقة هذا السلوك بالاستقرار على المستويات الوطنية والعالمية.

• تهديد الفضاء الإلكتروني لأنماط العلاقات الدولية

إنّ العلاقة بين الواقع الافتراضي والواقع الحركي للنظام الدولي يدفع من يمتلك القدرة إلى التوجه نحو الاستقطاب الإلكتروني بوصفه نمطًا جديدًا لتفاعلات العلاقات الدولية، من قبيل كثافة الولوج إلى الفضاء الإلكتروني وإلى مدى تتوافق فيه النظرة الإلكترونية للنظام الدولي مع الواقع الحركي لهذا النظام، وهذه الوضعية الهادفة للتوافق. ويمكن أن تنقسم صراعات الفضاء الإلكتروني على المستوى الدولي إلى الأشكال التالية:

1. الشكل الأول: يدور حول التحكم في الفضاء الإلكتروني الدولي.

2. الشكل الثاني: يدور حول تحويل القوة الافتراضية إلى مميزات استراتيجية.
3. الشكل الثالث: يتعلق بالصراعات الإلكترونية التي تحدد الأمن القومي للدول ذات السيادة.

وعلى سبيل المثال، ساعد الفضاء الإلكتروني في إنشاء أحلاف عسكرية إلكترونية، فقد أطلق حلف الناتو بقيادة الولايات المتحدة الأمريكية عام 2002 دعوة إلى تحسين قدراته الدفاعية ضد هجمات الفضاء الإلكتروني، وركز الحلف في السنوات التالية بشكل أساسي على تنفيذ تدابير الحماية السلمية المطلوبة للجانب العسكري، حيث دفعت هجمات الفضاء الإلكتروني التي وقعت في إستونيا عام 2007 الحلف إلى إعادة التفكير في حاجته إلى سياسة دفاع إلكتروني، ومن ثم وضع الحلف للمرة الأولى في تاريخه سياسة رسمية «للدفاع الإلكتروني» تم اعتمادها في يناير عام 2008، لتضع ثلاثة دعائم أساسية، أولها التضامن: بمعنى تقديم المساعدة عند الطلب، وخلاف ذلك يتم احترام مبدأ سيادة الدولة، وثانيها عدم التكرار: بمعنى تفادي الازدواجية غير الضرورية في الهياكل والقدرات على المستوى الدولي والإقليمي والوطني، وثالثها التأمين: من خلال التعاون القائم على الثقة، مع الأخذ في الاعتبار حساسية المعلومات ذات الصلة التي لا بد أن تكون متاحة، وأماكن الانكشاف الممكنة التي يمكن أن تتعرّض للاختراق بصورة أسهل.

وقد ساعد على تنامي مثل هذه التهديدات الإلكترونية لمصالح الدول، ومن ثم إمكانية بروز حروب سيبرانية، عدة سياقات أساسية مُحَفِّزة، من أبرزها (عبد الصادق، 2009: 155–161):

1. تزايد ارتباط العالم بالفضاء الإلكتروني، الأمر الذي اتسع معه خطر تعرض البنية التحتية الكونية للمعلومات لهجمات إلكترونية، فضلًا عن استخدامه من قبل الفاعلين من غير الدول، وخصوصًا الجماعات الإرهابية لتحقيق أهدافها التي تنال من الأمن القومي للدول.
2. تراجع دور الدولة في ظل العولمة وانسحابها من بعض القطاعات الاستراتيجية لمصلحة القطاع الخاص. وفي الوقت عينه تصاعدت أدوار الشركات متعددة الجنسيات، وخصوصًا العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء الإلكتروني، ولاسيما مع امتلاكها قدرات تقنية تفوق الحكومات.
3. نشوء نمط جديد من الضرر على خلفية الهجمات الإلكترونية يمكن أن تسببه دولة لأخرى، دون الحاجة إلى الدخول المادي إلى أراضيها. ذلك أن تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية جعل هذه الأخيرة عرضة للهجوم المزدوج، لما لها من سمات مدنية وعسكرية متداخلة، وخصوصًا أنّ الثورة التكنولوجية الحديثة تمخضت عنها ثورة أخرى في المجالات العسكرية وتطور تقنيات الحرب.

4. قلة تكلفة الحروب السيبرانية مقارنة بنظيراتها التقليدية، فقد يتم شنّ هجوم إلكتروني بما يعادل تكلفة دبابة، من خلال أسلحة إلكترونية جديدة ومهارات بشرية، علاوة على أنّ هذا الهجوم قد يتم في أي وقت، سواء أكان وقت سلم أم حرب أو أزمة، ولا يتطلب تنفيذه سوى وقت محدود.
5. تحول الحروب السيبرانية إلى إحدى أدوات التأثير في المعلومات المستخدَمة في مختلَف مستويات ومراحل الصراع المختلفة، على الصعيد الاستراتيجي أو التكتيكي العملياتي، بهدف التأثير بشكل سلبي في هذه المعلومات ونظم عملها.
6. توظيف الفضاء الإلكتروني في تعظيم قوة الدول، من خلال إيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة، وبذلك ظهر ما يسمى «الاستراتيجية السيبرانية» للدول، التي تشير إلى القدرة على التنمية، وتوظيف القدرات للتشغيل في الفضاء الإلكتروني، وذلك بالاندماج والتنسيق مع المجالات العملياتية الأخرى لتحقيق أو دعم إنجاز الأهداف عبر عناصر القوة القومية.
7. أدى تصاعد المخاطر والتهديدات في الفضاء الإلكتروني إلى بروز تنافس بين الشركات العاملة في مجال الأمن الإلكتروني بغرض تعزيز قدرة أسواق الإنفاق العالمي على تأمين البنى التحتية السيبرانية للدول، بالإضافة إلى بروز فاعلين آخرين من شبكات الجريمة المنظمة والقراصنة وغيرهم.

8. اتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون من الدول أو من غير الدول في الحرب السيبرانية، فقد تشنّ الدول الهجمات الإلكترونية عبر أجهزتها الأمنية والدفاعية، كما قد تلجأ إلى تجنيد قراصنة أو موالين لشنّ هجمات ضد الخصوم، دون أي ارتباط رسمي.

وقد عرف عالمنا المعاصر أول عاصفة إلكترونية جامحة من خلال ما أحدثته تسريبات «ويكيلكس» التي عرفت باسم «عاصفة ويكيلكس»، وتضمنت استخدام موقعها الإلكتروني في نشر صور ضوئية لآلاف الوثائق السرية الرسمية المتبادلة بين وزارة الخارجية الأمريكية وبعثاتها في دول العالم، وما أحدثته تلك التسريبات من توتر حاد في العلاقات الدولية على جميع الصعد، وما تسببت فيه من توتر العلاقات بين كثير من القادة والرؤساء والملوك في العالم، لما نسبته إليهم من اقوال وتصريحات تتعارض مع سياساتهم المعلنة تجاه شعوبهم، وهو ما أدى إلى حدوث اضطرابات واحتجاجات عديدة في هذه الدول.

وقد أدى اتساع علاقة الدول بالفضاء الإلكتروني، وما خلفته من حروب سيبرانية إلى جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، يمكن طرح أبرزها على النحو الآتي:

1. تصاعد المخاطر الإلكترونية، وخصوصًا مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم الإلكتروني عليها عبر وسيط وحامل للخدمات، أو شلّ عمل أنظمتها المعلوماتية، الأمر الذي يؤثر

في وظائف تلك المنشآت. وبالتالي، فإنّ التحكم في تنفيذ هذا الهجوم يُعدّ أداة سيطرة استراتيجية بالغة الأهمية، في زمن السلم أو الحرب.

2. تعزيز القوة وانتشارها، فقد عزز الفضاء الإلكتروني ما يُسمى «القوة المؤسسية» في السياسة الدولية، وهي تعني أن يكون لها دور في قوة الفاعلين، وتحقيق أهدافهم وقيمهم في ظل التنافس مع الآخرين، والإسهام في تشكل الفعل الاجتماعي في ظلّ المعرفة والمُحدِّدات المتاحة والتي تؤثر في تشكيل السياسة العالمية.

3. عسكرة الفضاء الإلكتروني، وذلك سعيًا لدرء تهديداته على أمن الفضاء الإلكتروني. وبرز في هذا الإطار اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن الإلكتروني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدى الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة.

4. إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول، وذلك عبر تحديث الجيوش، وتدشين وحدات متخصصة في الحروب الإلكترونية، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني، والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات الإلكترونية، والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء الإلكتروني، والقيام بمشروعات وطنية للأمن الإلكتروني.

5. الاستعداد لحروب المستقبل، حيث تبني العديد من الدول استراتيجية حرب المعلومات باعتبارها حربًا للمستقبل، يتم خوضها بهدف التشتيت، وإثارة الاضطرابات في عملية صناعة القرار لدى الخصوم، عبر اختراق أنظمتهم، واستخدام معلوماتهم ونقلها. وهنا ترى الدول الكبرى أنّ من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، بل القادر على شل القوة، والتشويش على المعلومة.
6. تحديث القدرات الدفاعية والهجومية، حيث سعت الدول إلى تحديث النشاط الدفاعي لمواجهة مخاطر الحرب السيبرانية، والاستثمار في البنية التحتية المعلوماتية وتأمينها، وتحديث القدرات العسكرية، ورفع كفاءة الجاهزية لمثل هذه الحرب عن طريق التدريب، والمشاركة الدولية في حماية البنية المعلوماتية، والاستثمار في رفع القدرات البشرية داخل الأجهزة الوطنية المعنية. وهنا يتعلق التوجه الأخطر بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع والتوتر مع دول أخرى (Martin، 2007 :1-9).

وهناك عاملان رئيسيان في انتشار رقعة الصراع في الفضاء الإلكتروني، وبالتالي إفساح المجال لنشوء الحروب السيبرانية، وهما:

أ. تغير منظور الحرب جذريًا، حيث انتقلت من نسق «الحروب بين الدول إلى وسط الشعوب»، فقد كان الغرض من الحرب قديمًا هو تدمير الخصم، إمّا باحتلال أرضه، أو الاستيلاء على موارده. أما

الحروب الجديدة فقد استهدفت بالأساس التحكم في إرادة وخيارات المجتمعات. ومن ثم ظهرت للشعوب الأهمية المحورية لهذا النمط الجديد من الحروب، سواء تعلق الأمر بالسكان المستهدفين في أرضية المواجهة، أو بالرأي العام في الدولة التي تشنّ الحرب، أو بالرأي العام على الصعيدين الإقليمي والدولي.

ب. بروز الصراعات ذات الأبعاد المحلية – الدولية، حيث ساعد اشتعال الصراعات الداخلية في مرحلة ما بعد الحرب الباردة، وكذلك طبيعة السياق الدولي للفضاء الإلكتروني، على توفير بيئة مناسبة لدمج الفئات والقوي المهمَّشة في السياسة الدولية، وخلق شبكة تحالفات مؤيِّدة أو معارضة ذات نطاق دولي عريض، إمّا على أساس قيم حقوقية، أو انتماءات عرقية أو دينية.

يسير التقدم التكنولوجي جنبًا إلى جنب مع سوق الأدوات والمهارات الذي يتوسع باستمرار، وهو ما يجعل أسلحة الهجمات الإلكترونية المعقدة متوفرة على الدوام، مثل البرمجيات الخبيثة والثغرات في الأنظمة المستهدَفة وما إلى ذلك، كما أنها توفر قدرات سايبرية قوية لأي فاعل (دولة أو ما دون الدولة) قادر على شرائها. ويفرض هذا الأمر تهديدًا على الاستقرار الدولي، مثلما يُسرِّع من عملية تسليح الفضاء الإلكتروني، وقد يطلق سباق تسلح سايبري تتنافس فيه الدول مع بعضها ومع الفاعلين من غير الدول.

• أنماط الصراع الإلكتروني الدولي وخصائصه

على الرغم من المميزات التي قدمتها الثورة الصناعية الرابعة التي يقودها الإنترنت وتقنيات الذكاء الاصطناعي، من حيث تحسين جودة ونمط الحياة، وزيادة فرص العمل، وسهولة التواصل بين الأفراد، كان لها تداعيات خطيرة أيضًا، حيث أظهرت أنماطًا مختلفة من التهديدات للأفراد أو الجماعات أو الدول، كما أنها غيّرت من أشكال الحكومات، فظهرت الحكومات الإلكترونية ثم الذكية، وغيّرت كذلك من مفاهيم إدارة العلاقات الدولية، فبدأ الحديث عن القوة الإلكترونية أو السيبرية، والحروب السيبرية، والصراع السيبري، والردع السيبري، والدبلوماسية السيبرية، وغيرها من هذه المفاهيم (خليفة، 2017: 63).

يدعم هذه الرؤية ملمحان، أولهما يخص الإمكانات الفائقة للقدرات السيبرانية في تشكيل تهديدات صريحة للخصوم، وهي تهديدات تتنوع ما بين شنّ حملات دعاية مغرضة، مرورًا بالتجسس السيبراني، واستخدام القدرات التكنولوجية في أعمال إرهابية، والتهديدات المسلحة غير المباشرة، وصولا إلى التهديدات العسكرية الصريحة، أمّا الملمح الآخر فيشير إلى أنّ امتلاك «القدرات السيبرانية» لم يعد حكرًا على فاعل بعينه، فقد أصبح في مقدور الدول الصغيرة والمتوسطة، والفاعلين من غير الدول كذلك (Non-State Actors)، مهما صغر حجمهم وتواضعت إمكانياتهم، الاستفادة من القدرات السيبرانية، بما فيها تطوير أسلحة رقمية، وتهديد الخصوم بها. وفي الوقت الحالي تتسع باطراد قائمة الدول

ذات القدرات السيبرانية المتطورة، فلم تعد القائمة تقتصر على القوى السيبرانية العظمى (عثمان،2017: 12).

وتتعدد أنماط الهجوم الإلكتروني باختلاف الأدوات التي يتيحها الفضاء الإلكتروني. ويمكن الإشارة إلى هذه الأنماط من حيث الاستهداف على النحو التالي (خليفة، 2017: 79):

أ. استهداف البنية التحتية المدنية المرتبطة بالفضاء: يتجه العديد من دول العالم إلى مكننة أنظمتها الخدمية وبنيتها التحتية، بهدف توفير الوقت والجهد والتمويل. وبالرغم من المميزات التي تقدمها المكننة الإلكترونية فإنها تجعل البنية التحتية عرضة للاختراق الإلكتروني.
فحينما تتعرّض البنية التحتية الحيوية لهجمات إلكترونية، فإنّ احتمالات كارثية يمكن أن تحدث، فمثلًا اختراق نظام المواصلات كأنظمة ملاحة الطيران والسفن وأنظمة السكك الحديدية والعبث بها، قد يوقع آلاف الضحايا في دقائق معدودة، كذلك فإن استهداف بعض القطاعات الحيوية، مثل مصافي البترول ومصانع الكيميائيات وأنظمة المستشفيات ومحطات توليد الكهرباء والمفاعلات النووية، قد تترتب عليه خسائر فادحة للدولة (Martin، 17:0072).

ب. تهديد البنى التحتية العسكرية المرتبطة بالفضاء الإلكتروني: مثّل فيروس ستوكسنيت على سبيل المثال، قفزة نوعية وكمية في القدرات المدمرة لحرب الفضاء الإلكتروني، فقد أعلنت الاستخبارات الإيرانية أن فيروس ستوكسنيت أصاب ما يقدر بستة عشر ألف جهاز كمبيوتر

نتيجة تعرّضها لهذا الفيروس في أكتوبر 2010، وتسبب في تعطيل نحو 1000 من أجهزة الطرد المركزي في منشأة ناتانز لتخصيب اليورانيوم، ما تسبب في تعطيل البرنامج النووي الإيراني مرحليًا،ولا يقتصر الأمر على تهديد البنى التحتية المدنية فحسب، بل شمل أيضًا البنى التحتية العسكرية، وهنا يطرح البعض تصورًا مستقبليًا حول إمكانية قيام فيروسات الكمبيوتر بإصابة نظم الدفاع الجوي ونظم توجيه الصواريخ والطائرات بدون طيار، بل وإمكانية إخراج الأقمار الصناعية عن مداراتها أو السيطرة عليها (خليفة، 2017: 80).

ج. سرقة المعلومات والبيانات العسكرية أو التلاعب بها: يتم في هذه الحالة اختراق الشبكات الخاصة بالمؤسسات الأمنية بهدف سرقة استراتيجيات عسكرية أو خرائط انتشار أنظمة تسليح، أو تصميمات لمعدات عسكرية، أو حتى قواعد بيانات عسكرية. وقد انطلقت واحدة من أخطر الهجمات ضد أنظمة حواسب الجيش الأميركي في عام 2008، من خلال وحدة تخزين بسيطة متصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة في الشرق الأوسط، ما شكل ما يشبه جسرًا رقميًا، تم من خلاله نقل آلاف الملفات من البيانات إلى خوادم خارجية، كما تم استهداف أكثر من 72 شركة، من بينها 22 مكتبًا حكوميًا، و13 من مقاولي وزارة الدفاع بهدف سرقة معلومات حول الخطط والمباني العسكرية.

ففـي تقريـر مقـدم إلـى الكـونغرس الأميركـي سُـرِّبت أجـزاء منـه إلـى صحيفة «واشنطن بوست»، ذُكر أن قراصنة صينيين يعملـون لمصـلحة الحكومـة الصـينية قـاموا بسـرقة معلومـات عسـكرية أميركيـة حـول منظومات مضـادة للصـواريخ مـن طـراز «PAC-3» ونظـام THAAD، إضافة إلى المعلومـات حـول الطـائرات والسـفن العسـكرية، مـا مكّـن الحكومـة الصـينية مـن اسـتخدام هـذه المعلومـات لتطـوير تقنياتهـا العسـكرية، وهـو مـا وفـر عليهـا الكثيـر مـن الوقـت والجهـد والأمـوال لتطوير هذه الأسلحة (Robert، 2013: 96).

د. اختراق أنظمة التحكم والسـيطرة: تكمـن الميـزة النسـبية لقـوة الفضـاء الإلكـتروني في قـدرتها علـى ربـط الوحـدات العسـكرية بعضـها بـبعض وبالأنظمة العسكرية، بما يسمح بسـهولة تبـادل المعلومـات وتـدفقها، وسـرعة إعطـاء الأوامـر العسـكرية، والقـدرة علـى إصـابة الأهـداف وتدميرها عن بعد. وقـد تتحـول هـذه الميـزة إلـى نقطـة ضـعف، إن لـم تكـن الشـبكة الإلكترونيـة المسـتخدمة في ذلـك مؤمنـة جيـدًا، منعًـا للتلاعـب بالأنظمـة العسكرية، أو إعـادة توجيـه أسـلحة الخصـم ضـد أهداف وهمية أو صديقة.

وفي الوقـت الـذي أعلنـت فيـه الصـين عـن إنشـاء وحـدات حـرب الفضـاء الإلكتروني عام 2003 تعرّضـت الولايـات المتحـدة في العـام ذاتـه لواحـدة مـن أسوأ حلقات التجسس الإلكتروني، وأطلق عليهـا اسـم «Titan Rain»، وتـم فيهـا سـحب مـا يـتراوح بـين 10 و20 تيرابايـت –وهـي وحـدة قيـاس لسـعة

التخزين في الكمبيوتر- من المعلومات من شبكة البنتاغون غير السرية، كما قام قراصنة إلكترونيون صينيون بشنّ بضع هجمات على المواقع الإلكترونية لشركة «لوكهيد مارتين» الأمريكية، وسرقوا معلومات عن تكنولوجيا تصنيع مقاتلة «إف -35» التي استخدمتها الصين في ما بعد لدى تصميم وتصنيع مقاتلة «تي 20» الصينية. وقد أطلقت الاستخبارات الأميركية على سلسلة من الهجمات التي شنّها القراصنة الصينيون عام 2007 تسمية «الجحيم البيزنطي»، وكانت الهجمات الإلكترونية تستهدف المؤسسات الصناعية الحكومية الأميركية (برم، 2010: 203).

أمّا من حيث مدى درجة شدة الصراع، فيمكن الإشارة إلى أنماط الصراع الإلكتروني على النحو التالي:

النمط الأول: حرب الفضاء الإلكتروني منخفضة الشدة

يتم استخدام الفضاء الإلكتروني كساحة للصراع منخفض الشدة، ويعبر هذا النمط عن صراع مستمر بين الفاعلين المتنازعين، وقد يكون ذا طبيعة ممتدة، ودائمة النشاط العدائي أو غير السلمي، بخلاف أنه عميق الجذور ومتداخل، وله نواح متعددة ثقافية أو اقتصادية أو اجتماعية، وعادة ما يتم اللجوء إلى القوة الناعمة للحروب السيبرانية في مثل صراعات كهذه، وإن كانت لا تتطور بالضرورة إلى استخدام القوة المسلحة بشكلها التقليدي، أو شنّ حرب إلكترونية واسعة النطاق (Richard، 2002: 548).

ولهذه الحرب السيبرانية الباردة وسائل عدة، منها شنّ الحروب النفسية، والاختراقات المتعددة، والتجسس، وسرقة المعلومات، وشنّ حرب الأفكار، والتنافس بين الشركات التكنولوجية العالمية وأجهزة الاستخبارات الدولية. وتجلى هذا النمط في حالات الحروب وفي الصراعات السياسية ذات البعد الاجتماعي - الديني الممتد، مثل الصراع العربي - الإسرائيلي، أو الصراع الهندي - الباكستاني، أو الصراع بين الكوريتين الشمالية والجنوبية، وغيرها (David، 2012: 188).

وفي مثل هذه الصراعات، تنشط جماعات دولية للقرصنة للتعبير عن مواقف سياسية أو حقوقية، مثل جماعة «ويكيليكس»، و«أنونيموس»، وكذلك في حالات الأزمات الدولية أيضًا، مثل التوتر بين إستونيا وروسيا في عام 2007، والاختراقات المتبادلة بين الصين والولايات المتحدة وروسيا، أو ما بين طهران وواشنطن. وقد تعرضت روسيا للاتهام بالقرصنة الإلكترونية في الانتخابات الأمريكية الأخيرة لدعم المرشح الجمهوري دونالد ترامب في مواجهة منافسته الديمقراطية هيلاري كلينتون، كما تم اتهام روسيا بشن هجمات إلكترونية على النرويج والتشيك وبريطانيا، مما دفع الدول الأخيرة لإعلان أنها قادرة على الرد بالمثل.

وقد شنت إيران أيضًا هجمات إلكترونية على منشآت نفطية في منطقة الخليج العربي، احتجاجًا على مزاعم بتعرض الأقليات الشيعية للتمييز،

منها هجمات فيروس «دوكو» في عام 2012، وهجمات فيروس «شمعون 2» ضد السعودية في يناير 2017 (خليفة، 2017: 73).

النمط الثاني: نمط حرب الفضاء الإلكتروني متوسطة الشدة

يتحول الصراع عبر الفضاء الإلكتروني إلى ساحة موازية لحرب تقليدية دائرة على الأرض، ويكون ذلك تعبيرًا عن حدة الصراع القائم بين الأطراف، كما قد يمهد لعمل عسكري. وهنا تدور حروب الفضاء الإلكتروني عن طريق اختراق المواقع الإلكترونية وتخريبها، وشنّ حرب نفسية ضد الخصوم، وغير ذلك (Diego، 2013: 16).

وتاريخيًا، تم استخدام الحروب السيبرانية متوسطة الشدة في هجمات حلف الناتو في عام 1999 على يوغوسلافيا، حيث استهدفت الهجمات الإلكترونية تعطيل شبكات الاتصالات للخصوم، وبرزت أيضًا خلال الحرب بين حزب الله وإسرائيل في عام 2006، وكذلك بين روسيا وجورجيا في عام 2008، والمواجهات بين حماس وإسرائيل في عامي 2008 و2012 (عثمان، 2017: 198).

النمط الثالث: حرب الفضاء الإلكتروني مرتفعة الشدة

يُعبّر ذلك النمط عن نشوء حروب في الفضاء الإلكتروني منفردة، وغير متوازية مع الأعمال العسكرية التقليدية. ولم يشهد العالم هذا النوع من الحروب، وإن كانت احتمالات حدوثها واردة في المستقبل مع تطور

القدرات التكنولوجية، واتساع الاعتماد بين الدول والفاعلين من غير الدول على الفضاء الإلكتروني.

وينطوي هذا النمط من الحروب على سيطرة البعد التكنولوجي على إدارة العمليات الحربية، حيث يتم استخدام الأسلحة الإلكترونية ضد منشآت العدو فقط، وكذلك اللجوء إلى الروبوتات الآلية في الحروب والطائرات دون طيار وإدارتها عن بعد، بخلاف تطوير القدرات في مجال الدفاع والهجوم الإلكتروني، والاستحواذ على القوة الإلكترونية.

وفي هذا السياق، يتم استخدام الفضاء الإلكتروني للاستعداد لحرب المستقبل أيضًا، عبر قيام الدول بتدريبات على توجيه ضربة أولية لحواسب العدو، واختراق العمليات العسكرية عالية التقنية، أو حتى باستهداف الحياة المدنية، والبنية التحتية المعلوماتية. والهدف من وراء ذلك تحقيق «الهيمنة الإلكترونية الواسعة» بشكل أسرع في حالة نشوب صراع (William، 2011: 15).

ومن هنا يمكننا استخلاص المراحل الأساسية التي تمر بها الهجمات الإلكترونية:

المرحلة الأولى: تتضمن طرق ووسائل الهجوم، وتشمل الهجوم بالفيروسات، والمساعدة في حرب المعلومات، أو المساعدة في الهجوم الإرهابي، أو تعطيل الخدمة، وغيرها من الوسائل.

المرحلة الثانية: تتمثل تلك المرحلة في إصابة الهدف، وهو البنية التحتية للمعلومات، الحكومات الإلكترونية، المصارف المالية، البورصات.

المرحلة الثالثة: تشمل التأثير الذي قد يكون له أبعاد داخلية وأبعاد خارجية.

المرحلة الرابعة: نتائج تلك الهجمات الإلكترونية وتداعياتها التي تشمل انهيار شبكات المعلومات، وإصابة المرافق الحيوية، والخسائر المادية والاقتصادية الهائلة، والارتباك العام.

وعلى صعيد آخر هناك معركة مشتعلة دائمًا بين صنّاع الفيروسات من جهة وشركات البرمجيات من جهة أخرى، فحينما ظهرت فيروسات الكمبيوتر واتضحت خطورتها، وبدأت شركات البرمجة في إنتاج برامج مضادة لها، تعمل على إزالتها ووقف نشاطها، تداعى صانعو الفيروسات، فقاموا بإنتاج فيروسات أكثر ضراوة وأخطر انتشارًا، إلى الحد الذي أصبح فيه الفيروس قادرًا ليس فقط على تدمير برنامج التشغيل، بل على استهداف المكوّن المادي للأجهزة الإلكترونية وإصابتها بالشلل. ويأتي تطوير أساليب وأنظمة أمن المعلومات – غالبًا – كرد فعل على هجمات إلكترونية ناجحة، ومن ثم تظهر الثغرات التي نفذت منها عملية الاختراق، وتبدأ مرحلة تأمينها. ولذلك كان من الضروري على الدول فصل شبكاتها الحرجة عن الإنترنت، ووضع نظام صارم لنقل البيانات والمعلومات خلالها، والتأكد من ولاء العناصر البشرية التي تعمل عليها،

والقيام بأساليب محاكاة لشنّ هجمات إلكترونية لمعرفة مواطن الضعف وتلافيها (محمود، 2013: 5).

وهناك العديد من النماذج التطبيقية على الهجمات الإلكترونية التي حدثت في الآونة الأخيرة، فمنذ عدة أشهر فرضت الولايات المتحدة الأمريكية عقوبات على شخصيات ومؤسسات من جمهورية كوريا الشمالية على خلفية الهجوم الإلكتروني على شركة (Sony Pictures Entertainment) بعد أن اتهمتها باختراق الشبكة المعلوماتية للشركة في 24 نوفمبر عام 2014، وسرقة بيانات شخصية لـ47 ألف شخص، وعرضت بطريقة غير شرعية خمسة أفلام من إنتاج الاستوديو، كما نشرت رسائل بريدية محرجة لمسؤولين فيه. ووصف محققون أميركيون متخصصون بالمعلوماتية الهجوم بأنه «غير مسبوق في طبيعته»، وأنه «الأكثر تدميرًا على الإطلاق على الأرض الأميركية». وأدى الهجوم عند حدوثه إلى تعطيل شبكة الشركة – وهي فرع للشركة اليابانية الأم– لمدة أسبوع، وإلغاء عرض فيلم (The Interview)، وهو فيلم كوميدي محوره مخطط متخيل لوكالة الاستخبارات المركزية الأميركية (CIA) لاغتيال الزعيم الكوري الشمالي كيم جونغ أون. ورغم نفي كوريا الشمالية لهذا الاتهام فإنّ الولايات المتحدة تمسكت بموقفها وقالت بأن لديها أدلة قوية على تورط كوريا الشمالية ومسؤوليتها عن هذه الجريمة.

وفي أغسطس 2009 قام الأمريكي ألبرت غونزاليس (28 عامًا) بسرقة بيانات لـ130 مليون بطاقة مصرفية، ونقلها إلى خوادم في أوكرانيا وهولندا

ولاتفيا، وقد تم وصف هذه العملية بأنها أكبر عملية نصب إلكتروني في تاريخ الولايات المتحدة من دون التطرق إلى الخسائر المالية المترتبة عليها (K.Saalbach، 2014: 26).

وفي يناير 2011 أعلنت الحكومة الكندية تعرض وكالاتها لهجوم إلكتروني ضخم، ومن بينها وكالة البحث والتطوير الدفاعي الكندية، وأجبرت الهجمات وزارة المالية ومجلس الخزانة الكنديين على فصل اتصالهما بالإنترنت (Peter، 2013: 2).

وفي أكتوبر 2012 اكتشفت شركة أمن المعلومات الروسية «كاسبرسكي» هجومًا إلكترونيًا عالميًا حمل اسم «أكتوبر الأحمر»، وقالت إنه يجري منذ عام 2007 على الأقل، ويعمل على جمع معلومات من سفارات وشركات أبحاث ومؤسسات عسكرية وشركات طاقة وغيرها، مشيرة إلى أنّ أهداف الهجوم الرئيسية هي دول في أوروبا الشرقية ودول الاتحاد السوفيتي السابق وآسيا الوسطى، وبعض دول أوروبا الغربية وشمال أميركا. وفي نفس العام 2012 قام شخص سعودي يدعى «أوكس عمر» باختراق خوادم سلاح الجو الإسرائيلي، وذكرت وسائل الإعلام الإسرائيلية أنّ عمر دخل بطريقة مفاجئة إلى الخادم الخاص بتدريب الطيارين بعد غياب لعدة أشهر، وحصل على كمية كبيرة من البيانات وصور الهويات والشهادات. وردًا على ذلك قام بعض المتخصصين الإسرائيليين في الإلكترونيات بالحصول على تفاصيل

آلاف بطاقات الائتمان السعودية، وهددوا بنشرها في حال استمرت الهجمات الإلكترونية لسعوديين على إسرائيل (برعام، 2013: 24).

وفي أبريل 2013 قامت مجموعة تعرف باسم «أنونيموس» بشنّ هجوم على مواقع إسرائيلية دعمًا للأسرى والقضية الفلسطينية، وشملت القائمة مواقع البورصة الإسرائيلية، ورئيس الوزراء، ووزارة الدفاع، وموقع جهاز الأمن الداخلي (الشاباك)، والصناعات العسكرية الإسرائيلية، إضافة إلى موقع مكتب الإحصاء الرسمي، وموقع وزارة التربية والتعليم، وعشرات المواقع الأخرى وآلاف الحسابات الإسرائيلية على موقعي فيسبوك وتويتر. وبالمقابل أعلنت مجموعة قراصنة إسرائيليين أنّها تمكنت من شنّ هجوم إلكتروني مضاد واختراق موقع «أنونيموس» (زكي، 2017: 55).

وظهرت مؤخرًا مجموعة تُعرَف باسم الجيش الإلكتروني السوري (Syrian Electronic Army) وهم مجموعة من قراصنة الإنترنت الذين يدينون بالولاء للنظام السوري ورئيسه بشار الأسد، ويستهدفون بالتالي مهاجمة أي مواقع إلكترونية لا تتفق مع آرائهم، أو يرون أنها معادية للنظام، أو تدعم الثورة الشعبية في سورية. وينسب للمجموعة نجاحها في اختراق عشرات المواقع الإلكترونية الإخبارية الشهيرة مثل: وكالة أسوشيتد برس الأميركية، ووكالة رويترز وصحيفة فايننشال تايمز البريطانيتين، وموقع منظمة هيومن رايتس ووتش الأميركية، وحتى موقع شركة البرمجيات مايكروسوفت، وغيرها الكثير. ويُعتبر الجيش

الإلكتروني السوري أول جيش افتراضي في العالم العربي يشنّ هجمات إلكترونية على خصومه بشكل صريح.

لقد أصبح الفضاء الإلكتروني ساحة لنقل الصراعات وتصفية الخلافات بشتى أنواعها بين الفرقاء، وفرض نفسه بقوة على واقع الصراعات المسلَّحة وغير المسلَّحة، وأضفت التقنيات الرقمية ومدى التقدم العلمي فيها مزيدًا من الفاعلية على ذلك النوع من الحروب عبر الفضاء الإلكتروني، إضافة إلى اتساع حجم ونطاق مخاطر تلك الأنشطة العدائية التي يمارسها الفاعلون في الحروب السيبرانية، والذين ينقسمون إلى فاعلين من الدول عبر أجهزتها الأمنية والدفاعية، وقراصنة تقوم الدول بتجنيدهم لتحقيق مكاسب سياسية، إذ يقوم الموالون والأتباع والمتعاطفون مع طرف ما بشنّ هجمات ضد من يرونه من الخصوم دون أي ارتباط رسمي من الدولة. وعلى الرغم من عدم تطوير الجماعات الإرهابية لقدراتها في الحرب الإلكترونية مقابل التطور في مجال القوة الناعمة، هناك مؤشرات على احتمالية تطوير الجماعات الإرهابية قدراتها الهجومية، ويمكن أن يكون تصاعد المخاطر والتهديدات ناجمًا عن قيام الشركات العاملة في مجال الأمن الإلكتروني بإشعال التنافس فيما بينها لتعزيز أسواق الإنفاق على الأمن السيبراني، بالإضافة إلى دور الفاعلين الآخرين من أرباب الجريمة المنظمة، والباحثين عن الشهرة من القراصنة والخبراء السابقين في الأمن الإلكتروني.

وعلى الرغم من أنّ العالم لم يشهد حربًا إلكترونية منفردة دون العمل العسكري التقليدي، هناك إرهاصات لحدوث ذلك في المستقبل. ويتميز هذا النمط من الصراع بتركيزه على سيطرة البعد التكنولوجي وهيمنته على إدارة العمليات الحربية، حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، ويتم استخدام الروبوتات الآلية في الحروب والتي يتم إدارتها عن بعد فضلًا عن الطائرات دون طيار، ويتم تطوير القدرات في مجال الدفاع والهجوم الإلكتروني والاستحواذ على القوة الإلكترونية. كما يتم استخدام الفضاء الإلكتروني في الاستعداد لحرب المستقبل والقيام بتدريبات على توجيه ضربة أولى لحواسب العدو، واختراق العمليات العسكرية عالية التقنية، أو حتى باستهداف الحياة المدنية والبنية التحتية المعلوماتية. ولعل الهدف من وراء ذلك تحقيق «الهيمنة الإلكترونية الواسعة» بشكل أسرع في حالة نشوب صراع (عبد الصادق، 2012: 185).

وقد لعب الفضاء الإلكتروني دورًا في إعادة تشكيل القوة القومية للدولة على أسس جديدة يمثل البعد الإلكتروني بعدًا جوهريًا في تكوين عناصرها وتماسكها واستمراريتها، بالإضافة إلى تغيير مقاييس القوة التي كانت تركز بالأساس على الموارد الطبيعية وحجم السكان والمساحة الجغرافية. وتم إضافة القدرة على استحواذ القوة الإلكترونية، وأثر الفضاء الإلكتروني في عناصر القوة القومية، فللصراع الإلكتروني مجموعة من الخصائص التي تميزه وهي (خليفة، 2016: 28):

1. الفاعلون الدوليون متنوعون، وفي بعض الأحيان مجهولون.
2. سهولة الابتداء والانتهاء.
3. في الصراع الإلكتروني جزء مادي يتمثل في خضوع الأجهزة والخوادم والحاسبات لسلطان الدولة وسيادتها.
4. قابلية تغيير خصائصها مستقبلًا، نتيجة التغييرات السريعة في التكنولوجيا.
5. الغالبية العظمى لا تستطيع نزع سلاح الطرف الآخر أو تدميره كليًا أو احتلال إقليمه.
6. إمكانية استخدام الفضاء الإلكتروني في القوة الناعمة أو الصلبة.

• الشرق الأوسط والصراع الإلكتروني

تُعدّ منطقة الشرق الأوسط مهمة جدًا في سلّم الاستراتيجيات الدولية، ليس الآن فقط، بل منذ أن اتخذ الصراع الدولي بين الدول قدرته على التأثير في المحيط الخارجي لسلطته، فهذه المنطقة كانت في تاريخها القديم مسرحًا لصراعات الأقوياء من الأفراد والجماعات والدول، وبالشكل الذي جعلها كتلة ترجيحية لمن يستطيع أن يمسك بقلاعها النشطة تأثيرًا وفعلًا، مما مكن القادر منهم من أن يتسيد في زمانه، فهذه المنطقة هي خزان العالم الكبير من الثورة النفطية التي يحتاجها الجميع الآن وفي المستقبل، إضافة إلى أهميتها الجيوستراتيجية، وكونها منطقة مليئة بالعقائد والأديان والمذاهب والقوميات والطموحات والمطامع،

مما جعلها مرجلًا فوّارًا في كلّ وقت، وهو ما يمنحها تأثيرًا حاسمًا في مجمل صراعات الأقوياء، وهذا ما أضفى مستوى عاليًا من أشكال إدارة الصراع ومستوياته على الصعد كافة.

وتشهد المنطقة العربية خصوصًا – ومنطقة الشرق الأوسط بالشكل الأعم – اندفاعات وتباينات مختلفة ومتعددة، تؤثر بشكل كبير في قراءة ما يحدث في المنطقة من تغييرات بعضها عميق وذو تأثير مستقبلي. وفيما يخص شكل تعامل دول المنطقة مع الفضاء الإلكتروني، أخذ الأمر مهمتين متقاطعتين:

الأولى: الرغبة الكبيرة في التعامل مع هذه التقنية وما تقدمه من خدمات لغرض التطور والتقدم، والتعامل مع الجديد من العلم.

الثانية: تحصين الجدار الوطني من اشتباكات الاختراق والتسلل الذي تتعرض له دول المنطقة من دول ذات إمكانات تقنية عالية بحكم الاختلاف السياسي المُعبَّر عنه بسلوكيات سياسية مطبقة على الأرض.

وقد تداخلت المهمتان معًا من أجل دفع الأضرار أو تقليلها في الأداء السياسي والاقتصادي والعسكري والعلمي لدول المنطقة، مما استوجب إطارات متجددة لهذه الحرب التي تتطور أساليبها بشكل سريع ومتجدد، ولا سيّما أنّ هذه المنطقة شهدت حروبًا متعددة، مما جعلها أشبه بمختبر للجديد من هذا العلم، فقد أطلقت حرب عاصفة الصحراء عام 1991 الثورة في التقنية العسكرية، محدثة نتائج هائلة في مجرى الحروب وفي التوظيف الاستراتيجي الداعم لسياسات الدول. ويشير أحد القادة

الميدانيين ممن اختبروا تلك التقنية في ميدان المعركة في الشرق الأوسط إلى أنّ عصر «الاختراقات في التقنية العالية تضاعف بسرعة، ومع نضج عصر المعرفة في العالم، صار مفهوم «فضاء المعركة حقيقة واقعية»» (علي، 2014: 58).

دأبت الولايات المتحدة الأمريكية - بوصفها أكثر الدول المعنية بمنطقة الشرق الأوسط لثرواتها وموقعها الجيوستراتيجي، فضلًا عن حماية أمن «إسرائيل» - على التدخل في كلّ شؤون المنطقة، تعويقًا وتعطيلًا واختراقًا، وصولًا إلى شنّ الحروب عندما فشلت أساليبها الأخرى، مثلما حصل في عدوانها على العراق عام 2003، فقد كُلِّفت وكالة الأمن القومي الأمريكية «NSA» بمهمة الإطلالة الدقيقة على ما يحدث في المنطقة من تطور وتقدم في هذا الشأن، وتزايد اهتمامها بهذا النشاط في المجمع الاستخباري الأمريكي بعد الحرب الباردة، بسبب طبيعة التطورات التقنية والإلكترونية التي باتت جزءًا أساسيًا من مهام الوكالة التي تؤدي دورًا استراتيجيًا في موضوع الأمن القومي الأمريكي، من خلال طبيعة ما يسمى الإرهاب الإلكتروني القائم على أساس تشويش المعلومات والنظم التي تؤثر بشكل كبير في الأنظمة المعلوماتية، إذ إنّ اختراق بعض البيانات والقواعد المعلوماتية وإفسادها، يؤثر في الهيكل التنظيمي الذي تقوم عليه المؤسسات الأمريكية في هذا الجانب، مما يدعو إلى اعتباره تهديدًا، وهو ما يجعل من الوكالة ذات أهمية كبيرة في هذا الشأن.

وقـد دخلـت المنطقـة منـذ انتهـاء الحـرب البـاردة مرحلـة الحـرب الإلكترونية التي دشنتها الولايات المتحدة، أولًا ضد العراق في حرب عام 1991، ومن ثم في فترة الحصار التي امتدت أكثر مـن 12 عامًـا، وأدت فيهـا فـرق التفتـيش الدوليـة دورًا فـاعلًا ومـؤثرًا في اخـتراق كامـل المنظومـة السيادية العراقية بتقنياتها المتطورة وأجهزتها الحساسة والدقيقة. ومـن ثـم ثنَّتها ضد إيران بمعونة إسـرائيلية واضـحة، ممـا جعـل مـن فضـاء المنطقـة مسرحًا لحروب إلكترونية متواصلة ومتجددة.

وقد باتت هذه الحرب في الحقيقة أمرًا واقعيًا وملموسًا، ولا سيّما بعـد أن هاجمت فيروسات مثل «Stuxnet» و«Flame» العديد من المصـارف، ثم طالت منشآت نووية إيرانية وشركات نفط سعودية وقطرية، ممـا سبب إرباكًـا وتعطـيلًا وتلفًـا لكـلّ مـا طالـه هـذا الفيـروس، وقـد مثّـل فـايروس «Stuxnet» – بشكل لـم يسبق له مثيل – القدرة على شـنّ الهجمـات علـى ثلاث مراحل أو أطـوار، ففـي المرحلـة الأولـى يسـتهدف الآلات العاملـة على نظام «Microsoft windows» وشبكاتها بحيث يدفعها إلى أن تكـرار إعادة نسخ ذاتها، ثم تتوجه إلى برنـامج «Siemens step 7 » الـذي أساسـه «Windows» أيضًا، والذي يستخدم نظم التحكم الصناعية البرمجية التـي تُشـغِّل المعـدات كـأجهزة الطـرد المركـزي، ثـم يقـوم أخيـرًا بالمسـاس بالمتحكمات المنطقية المبرمجة (السيد، 2016: 5).

وبهذا التحكم التكاملي والمتبادل تمكـن مخترعـو هـذا الفيـروس مـن التجسـس علـى المنظومـات الصـناعية، وحتـى التسـبب في جعـل أجهـزة

الطرد المركزي سريعة الدوران، مما يدفعها إلى أن تمزق ذاتها، حيث يستطيع هذا الفيروس الانتشار بخفة بين أجهزة الكمبيوتر التي تُشَغّل «Windows» حتى ولو كانت غير متصلة بالإنترنت، فإذا قام أحد العمال بوضع شريحة «ups» داخل آلة أدى ذلك إلى إصابتها بعدوى هذا الفيروس مما يمَكّنه من الانتشار داخلها، ومن ثم إلى الآلة التالية التي يمكنها قراءة ما هو موجود داخل شريحة «ups». ولأنّ بمقدور كلّ شخص إصابة مثل هذه الآلات بهذه الوسيلة دون إثارة أي شكوك أو شبهات، فإنّ إمكانية انتشارها داخل الشبكات المحلية أمر متاح وسريع التحقيق.

وقد انتبهت إيران إلى إمكانات الفضاء الإلكتروني، ووعت مخاطره عام 2009 حينما استخدم محتجون مناهضون للحكومة خدمة الإنترنت لتنظيم الاحتجاجات ضد نتائج الانتخابات الرئاسية التي أوصلت «محمود أحمدي نجاد» إلى سدة الرئاسة، ومنذ ذلك التاريخ أوكِلَت مسؤولية هذا الأمر إلى الحرس الثوري الإيراني، من خلال مراقبة الإنترنت، وحجب بعض المواقع وتعطيل أخرى، وكانت الموارد المالية المخصَّصة لهذه الحرب كبيرة، وبدعم من أعلى السلطات.

إنّ الفضاء الإلكتروني هو المجال الذي ستتحرك نحوه المواجهة، فطهران تجده حافظة أساسية في ترسيخ الأمن الوطني، ودفاع صدّ أمام المتسللين على خصوصياتها، ولا سيما أنّ الطبيعة المتداولة عن النظام السياسي تركن إلى السرية والتخفي وإنكار كلّ ما يراه الآخرون تسللًا أو

تدخلًا أو تعويقًا، ولذلك فقد باتت الإجراءات الإيرانية في هذا الجانب متسارعة مع ما تتصف به من توجس وقلق وارتياب بما يحصل بالضدّ منها، خشية انكشافها لخصومها (جواد، 2016: 137).

أمّا إسرائيل التي تُعدّ كيانًا استيطانيًا مزروعًا في المنطقة على حساب شعوب أخرى، مع ما تتصف به من عدوانية منفلتة، فإنّها تجد نفسها في حرب متعددة الأشكال مع المحيط العربي الإسلامي، وهو ما يدفعها إلى أن تكون طرفًا فاعلًا في المبادرة لشلّ وتعطيل قدرات الآخرين المعادين لها. وقد أكد خبراء عالميون في مجال المعلوماتية بأنهم يعتقدون أنّ الاستخبارات الأمريكية - بالتعاون مع الاستخبارات الإسرائيلية - هي التي طورت فيروسي «Stuxnet» و«Flame» اللذين هوجمت بهما إيران في الكثير من مفاصل شبكتها الوطنية ومواقعها الحساسة، ولا سيّما العسكرية والنووية والنفطية. وذكر هؤلاء أنّ الفيروسات صارت أقوى سلاح في هذه الحرب التي أعلنتها الحكومة الأمريكية ضد إيران. كما لم يعد سرًا حجم وعمق التعاون الأمريكي - الإسرائيلي في هذه الحرب، لأنّ بعض الخصائص المشتركة بين «Stuxnet» و «Flame» توحي بأنّ الدولة التي تقف وراء فيروس «Stuxnet» تقف أيضًا وراء «Flame»، لأنّ من الممكن استخدام فيروسين يعملان على البرنامج نفسه، ولكن باستخدام نهجين مختلفين (السعدون، 2012: 18).

وقد تبادلت الأطراف الداخلة في هذه الحرب أنماطًا من الهجوم المضاد ضدّ بعضها بعضًا، حيث تعرضت الكثير من المواقع الإسرائيلية

الإلكترونية إلى العديد من الهجمات المنسقة التي استهدفت تعطيل أو اختراق الكثير من المؤسسات الرسمية الإسرائيلية، ردًا على ما كانت تقوم به من دفعات هجومية مصممة ضد الأطراف الأخرى، وفي المقدمة من ذلك إيران. وقد تبنت تلك الاختراقات مجموعة القرصنة الإلكترونية «أنونيموس» التي أشارت إلى أنها ستكرر محاولاتها في أي وقت تراه مناسبًا للاختراق (علي، 2014: 103).

إنّ الحرب الإلكترونية التي تمارسها «إسرائيل» ضد عموم بلدان المنطقة استهدفت، حتى في جوانبها العسكرية، دولًا مثل «مصر وسورية والأردن والعراق والسعودية وتركيا... الخ»، وغايتها في ذلك تحصين قدراتها الإلكترونية تحسبًا لأي طارئ يُعرِّض أوضاعها للخطر، وهي تطبق في هذا الاندفاع ما يسمى مفهوم الحرب الاستباقية، مستندة في ذلك إلى ما تتمتع به من قدرات علمية ومعلوماتية متقدمة قياسًا إلى ما يمتلكه الآخرون في المنطقة. فإسرائيل ومعها الولايات المتحدة الأمريكية تخشى من التقدم السريع الذي تحققه إيران والأطراف الشرق أوسطية الأخرى في مجال الحرب الإلكترونية بشقيها الهجومي والدفاعي، ولذلك تقوم بمراقبة ما يحصل وتدقيق نتائجه بوصفه أمرًا أكثر من ضروري، لأنه يتيح لها الوصول إلى مقاربات أقرب إلى الدقة في قراءة ما يُخطَّط ضدّها. مع تقديرنا أنّ الجميع يفضل خيار المجابهة الإلكترونية لأنها أقل تكلفة اقتصاديًا وعسكريًا من الحرب التقليدية.

وفي المقابل، فإنه عندما تحركت شعوب عربية ضد الحكام الدكتاتوريين الذين سيطروا عليها لعقود من الزمن، فيما أصبح يسمى بالربيع العربي، كان الإنترنت الحليف التكنولوجي الذي مكّن الناس من تبادل المعلومات وتنظيم التظاهرات، والترويج للحركة بأسرها. وقد فُتِح نقاش واسع حينئذ بشأن القرصنة الإلكترونية، فبعدما اعتاد الخطاب العربي السائد تصوير الهاكرز على أنهم شباب مهووسون تقنيًا، ويقضون وقتهم في محاولة اختراق أمن الدول والمؤسسات الكبرى من باب التسلية فحسب، جاءت الانتفاضات الشعبية العربية التي اندلعت في المنطقة العربية لتبين أنّ كثيرًا من عباقرة الحاسوب هؤلاء يستعملون خبراتهم لمساعدة الثوار وفضح الحكومات، مثل مساعدتهم المواطنين المصريين في إيجاد حلّ مكّنهم من استعمال مواقع التواصل الاجتماعي، عندما أمرت حكومة الرئيس السابق حسني مبارك بتعطيل خدمات الإنترنت، كما ساعدت المحتجين الليبيين واليمنيين، وقام أعضاء من «الأنونيموس» بقرصنة المواقع الرسمية التابعة لنظام الرئيس التونسي السابق زين العابدين بن علي، ردًا على حجب الإنترنت في بداية الثورة.

وقد اجتمعت عوامل مباشرة تتعلق بالانفجار السكاني في الوطن العربي، وانهيار الطبقة المتوسطة وانهيار قدرتها الشرائية، وحرمان قطاعات كبيرة من الشباب من الفرص السياسية أو الاجتماعية أو الاقتصادية، وهو ما مثّل بدوره عوامل متراكمة للاحتقان الشعبي وضعف الثقة بين الدولة والمجتمع، ليشكل فيما بعد بيئة حاضنة لاستيعاب

«الوضعية الثورية» التي تمثلت في سلسلة كبيرة من المظاهرات والاحتجاجات السلمية ضد النظم قبل اندلاع الثورات في نهاية عام 2010 وبداية عام 2011. وكان من أبرز ذلك ظهور حركات احتجاجية مثل حركة «6 أبريل» وحركة «كفاية» ومنظمات المجتمع المدني. وجاءت شرارة الموجة من تونس، ثم حدث تمدد إقليمي لها في ظروف مشابهة. وحدث التغيير في بعض الدول نتيجة حراك سياسي داخلي مثل مصر وتونس، وكان للخارج دور في بعضها الآخر، من خلال المساهمة في الصراع، والتعجيل في سقوط النظام، مثل حالة التدخل العسكري المباشر لحلف الناتو في ليبيا، والدعم غير المباشر للمعارضة المسلحة في سورية. ومن جهة أخرى شهدت دول مثل البحرين احتواءً للمعارضة بدعم مجلس التعاون الخليجي، وحدث في بعض الدول تغيير في سياسات النظام بمبادرة من أعلى مثل المغرب والجزائر.

وبرز في تلك التغييرات دور شبكات التواصل الاجتماعي في الدعوة إلى المظاهرات، وتدشين صفحات باسم الثورة والدعوة إليها وطلب التفاعل والمشاركة، وبرز دور الشبكات الاجتماعية والإنترنت بصفة عامة في التغيير. وعكس ذلك من ناحية أخرى التحول إلى نمط جديد من جماعات الضغط الإلكترونية التي انتقلت من مجرد التأثير على السياسات العامة إلى القدرة على إحداث انفجار شعبي نجح في إسقاط النظام السياسي برمّته (الخوري، 2011: 153).

وهناك العديد من الأبعاد التي عززت دور الفضاء الإلكتروني في ثورات الربيع العربي منها (عبد الصادق، 2012: 137):

1. بعد مؤسسي: يتمثل في ضعف دور الأحزاب السياسية والمجتمع المدني وممثلي السلطة التشريعية، كمؤسسات وسيطة بين الحاكم والمحكومين، وعجزها عن حمل مطالب الرأي العام، مما أدى إلى انفصال تلك المؤسسات عن الواقع الاجتماعي والسياسي الذي تعيش فيه، بالإضافة إلى عدم التوافق بين التغييرات في الرأي العام وعملية وضع السياسات.
2. بعد تكنولوجي: يتمثل في الارتباط المتزايد بتكنولوجيا الاتصال والمعلومات، وتوفير فرص أمام لاعبين جدد، وخصوصًا مع ما وفره الإنترنت من وسيلة سهلة ورخيصة وسريعة الانتشار، وكذلك اندماج الخدمات بعضها ببعض، حيث يتيح الإنترنت خدمة الاتصال، ويتيح الموبايل خدمة الإنترنت وإمكانية التراسل المجاني بينهما، فضلًا عن الحرية المتاحة وارتفاع سقفها عن سقف وسائل الإعلام التقليدية.
3. بعد تنموي: إنّ المجتمعات التي تكون في طور التحول يكون لديها حالة متصاعدة من الحراك السياسي، وقد شهد المجتمع العربي عددًا من السياسات التي تشكل دورًا هامًا في إيجاد حالة من الحراك السياسي بين المهتمين بالشأن العام، بالإضافة إلى أنّ انفتاح المواطن على الخارج جعل لديه طموحات وتطلعات أكبر، قد تمثل ضغطًا مستمرًا على صانعي القرار في ظل قيود الواقع الاجتماعي

والاقتصادي، وقد زادت تلك الضغوط بعد تنحي الرئيس التونسي زين العابدين بن علي.

4. بعد ذو طابع حيوي (جيلي أو عمري): ينطلق من أنّ الشباب في العالم العربي يمثلون ما يقرب من 60٪، وهم الفئة الأكثر معاناة وفاعلية، وتمثل كتلة حرجة للتغيير.

لقد أحدث الفضاء الإلكتروني انتشارًا للقوة السياسية داخل المجتمع الدولي من قِبل فاعلين خارج نطاق النظام السياسي الرسمي الذي تسيطر عليه الدول، وهو ما أدى إلى وجود نمط جديد من العلاقة بين المؤسسات داخل النظام السياسي والمؤسسات الخارجية، ودخل في صناعة القرار السياسي الدولي فاعلون آخرون غير القادة وزعماء الدول أو المؤسسات السياسية المحلية التقليدية، أو المؤسسات الدولية التي تسيطر عليها الحكومات في عضويتها، وجاء ذلك متزامنًا مع تعرُّض الدولة القومية لتآكل سيادتها، وفقدانها السيطرة على سياستها الإعلامية وقدرتها على تعبئة الرأي العام العالمي. وتدرك الأطراف الداخلة في هذه اللعبة أنّ الحرب الإلكترونية هي اشتباك غير معلن، وهي تجري بصمت وهدوء، فلا جبهات مُعلَنة ولا أطراف تتبنى الهجمات، لأنّ ما يحصل لا تنظمه اتفاقيات مُعلَنة أو قواعد اشتباك جرى التعامل بها، ولذلك ستظل هذه الحرب مستمرة ومتعددة الأغراض، ما دامت برامج الأطراف الداخلة فيها مختلفة، وما دام العلم يقدم من الأدوات ما يحرض على الاستمرار بالمواصلة.

وما تزال القواعد الحاكمة في الفضاء الإلكتروني أبعد ما تكون عن الوضوح، بل إنّ ما يحصل فيه أقرب إلى الحرب الصامتة بين المتخاصمين، وهذا ما يمنح اللاعبين فيه القدرة على الإنكار والنفي بخصوص أية أضرار تقع على الطرف الآخر، حتى وإن كانت تمس الأمن الوطني. مع تقديرنا أنّ هذه التكنولوجيا تتجاوز إلى حد بعيد المناقشات المفتوحة بشأن استخدامها بأشكالها المعروفة. ويتيح ذلك للدول في الوقت الراهن ألّا تضع على نفسها قيودًا كثيرة في الفضاء الإلكتروني، وهذا أمر يشكل خطورة لأنّ تداعياته ونتائجه قد تفضي إلى نزاع يصل إلى حد «الحرب»، ولكنها – وللمفارقة – حرب لا تعلن عن نفسها، ونادرًا ما تكون مرئية، رغم أنها مستمرة بشكل فعال. ويضاف إلى ذلك أنّ هذه الحرب الصامتة والافتراضية تنطوي على درجة من الضغائن وانعدام أخلاق النزاع، يشعر حيالها المرء بأنّ الدول تكشف فيها عن أحقادها على نحو سهل لعدم وجود حسيب أو رقيب يسجل ذلك. فالقاتل الافتراضي كما الضحية الافتراضية هو مما لا تعلن عنه الدول، أي لا اعتراف بحجم الخسائر، ولا رغبة في كشف النية، وفي ذلك مخاطر جمة على مستوى العلاقات الدولية والمجتمع الدولي، لأنّ المهاجم والمتعرض للهجوم أدوات صماء، بإمكانها أن تخرب وتدمر الطرف المقابل دون رادع من ضمير أو أخلاق.

لم تعد تكنولوجيا الاتصال والمعلومات تُستخدم للتعبير عن حالات الصراع فقط، بل أصبحت هي ذاتها ساحة للصراع، كما أنها تستخدم في

حل تلك الصراعات وتسويتها. وقد تغيرت أساليب الصراع مع ثورة التكنولوجيا والمعلومات، وأصبح الصراع التقني هو الأكثر ظهورًا، وساهم الطابع التكنولوجي في إيجاد طرق جديدة للصراع، بديلة عن الحرب المباشرة بين الدول، حيث ساهمت الآليات التكنولوجية في مساعدة المنظمات والدول في التنسيق بين جهودها والتفاعلات فيما بينها إلكترونيًا بعيدًا عن الاتصال المباشر، وأدت الثورة التكنولوجية إلى تغير شكل الحرب وأدواتها والفاعلين فيها، مما ساعد على اختلاف درجة التهديد وآثاره وطبيعته ومصادره وظهور حرب الشبكات وحروب الفضاء الإلكتروني.

الخاتمة

نجد من خلال ما سبق أنّ التكنولوجيا أصبحت تلعب دورًا بارزًا في الصراعات الدولية، وتحظى باهتمام صانعي القرار الاستراتيجي منذ عقود الحرب العالمية الأولى، فقد غدت علاقة التقدم التكنولوجي بصناعة القرار الاستراتيجي علاقة حتمية، وأدى اتساع علاقة الدول بالفضاء الإلكتروني، وما خلفته من حروب سيبرانية، إلى ظهور جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية.

نتائج الدراسة:

1. إنّ التطورات التكنولوجية غيرت من الأشكال التقليدية للقوة، وأدخلت مفاهيم جديدة لم تكن موجودة من قبل، وظهر نوع جديد من القوة هو القوة الإلكترونية التي تعمل إلى جانب الأشكال التقليدية للقوة الصلبة منها والناعمة، وأصبحت إحدى أهم أدوات تحقيق السياسة الخارجية للدول، بل والسياسات الداخلية أيضًا.
2. ازداد توجه الدول بعد الحرب العالمية الثانية إلى مبدأ الحرب المحدودة الذي يعتمد على استخدام الأسلحة التكتيكية الصغيرة، بدلًا من الانتقام الشامل الذي كان يعتمد على مبدأ الردع النووي فقط، فقد أضفى التقدم التكنولوجي العسكري مزيدًا من المرونة، وسعت الدول إلى تصميم أنواع محدَّدة من الردود العسكرية في مواجهة مختلف التحديات التي تواجهها.
3. تطور الأمر إلى استخدام الأقمار الصناعية التي تُعدّ إحدى أهم تطبيقات الحرب الإلكترونية في حرب الخليج عام 1990 والحروب العربية

الإسرائيلية، لأغراض الاتصالات والملاحة والاستخبارات، والمخصصة للاستخبارات الإلكترونية التي زودت القادة الميدانيين بالمعلومات الفورية، إضافة إلى استخدام العديد من تدابير المساندة الإلكترونية الأخرى كالتشويش على ترددات الاتصالات اللاسلكية، والطائرات دون طيار المجهزة بجهاز تصوير فيديو وجهاز مسح إلكتروني يعمل بالأشعة فوق الحمراء، لتوفير بيانات تكتيكية قتالية حقيقية.

4. تم إدخال الطائرات دون طيار المخصصة للمراقبة والمطاردة والقتل، والروبوت العسكري ذي الإمكانيات التكنولوجية العالية في الحرب على الإرهاب منذ غزو العراق عام 2003، كأحدث الأدوات العسكرية في الحرب الإلكترونية، التي أحدثت طفرة في مجال الثورة في الشؤون العسكرية نتيجة لتمتعها بالذكاء الاصطناعي، وقدرتها على التحرك في مختلف الأجواء المناخية والتضاريس.

5. إنّ هذه الأدوات والوسائل التقنية والرقمية التي تتسلح بها الحرب الإلكترونية، وتحديدًا في القطاعات العسكرية التي شهدت تطورات عديدة، جعلتها تعتمد بشكل مباشر على عنصر المعلوماتية والرقمية، وحوّلتها إلى بنى تتسلح بأجيال جديدة من الأسلحة التكنولوجية والاتصالية، وزادت من قدرتها وفاعليتها على الدعم اللوجستي والتواصل المعلوماتي والاستخباراتي القائم على توفر عنصر التقنية الحديثة، وهو ما أضفى على الوسائل والأدوات العسكرية والحربية قدرًا كبيرًا من الدقة والجاهزية، وجعل الصراعات الدولية تعتمد بشكل كبير على فوارق امتلاك هذه الأدوات وقدرات استخدامها، في تحديد مستوى الصراع أو الطرف المنتصر فيه .

6. جاءت الطفرة العالمية في مجال انتشار تكنولوجيا الاتصال والمعلومات لتطرح الكثير من التأثيرات على الصراعات الدولية، وبرزت ظاهرة الفضاء الإلكتروني مع التطور في مجال التطبيقات والاستخدام، وحجم الانتشار والتأثير لتكنولوجيا الاتصال والمعلومات في المجتمع الدولي، وهو الأمر الذي ساعد في تبلور ظاهرة الفضاء الإلكتروني كمجال جديد في الصراعات الدولية، وهو ما عمل على إحداث مجموعة من المتغيرات في نطاق العلاقات الدولية على مستوى التطبيق، شملت مستوى التحليل ووحدة التحليل، فقد ساعدت حرب الفضاء الإلكتروني على ظهور فاعلين دون مستوى الدولة كالقراصنة الإلكترونيين أفرادًا ومجموعات، وهو ما أثّر بشكل كبير في بنية النظام الدولي واتجاه التفاعلات فيه.
7. فرض الفضاء الإلكتروني إعادة التفكير في مفهوم الأمن كإحدى أهم قضايا المجتمع الدولي، لأنّ زيادة اعتماد الدول على شبكات الإنترنت ترفع من احتمالية تعرضها لهجمات إلكترونية تهدد أمنها، من خلال استهداف البنى التحتية الاستراتيجية لهذه الدول، وتزيد أيضًا من التحديات المرتبطة بأمن المعلومات الإلكتروني، والمتمثلة في التحديات السياسية والاقتصادية والتقنية والأمنية. وقد أدخلت حرب الفضاء الإلكتروني دول العالم في هاجس أمني قوي، وخصوصًا أنّ هذه الدول قد قامت بوضع مدخراتها القومية على شكل معلومات رقمية عبر فضاء مذاب الخصوصية، وضعيف الأمن بالنسبة إلى بعض الدول، وفائق السرعة، وزنبقي الشكل، مما زاد من الفجوة المعلوماتية القومية بين الدول.
8. يمكن لقوات حرب الفضاء الإلكتروني أن تدخل في قلب هذه الشبكات وتسيطر عليها أو تدمرها، وإذا استولت على شبكة ما يمكنها أن تسرق كلّ

معلوماتها، أو ترسل إليها تعليمات بتحويل الأموال، أو تسريب النفط، أو إطلاق الغاز، أو تفجير المولدات، أو إخراج القطارات عن قضبانها، أو صدم الطائرات، أو إرسال كتيبة لتقع في كمين، أو تفجير قذيفة في المكان الخطأ، الأمر الذي أدى إلى دخول المجتمع الدولي في مرحلة جديدة تلعب فيها هجمات الفضاء الإلكتروني دورًا أساسيًا في تعظيم القوة أو الاستحواذ على عناصرها الأساسية. وأصبح التفوق في مجال الفضاء الإلكتروني عنصرًا حيويًا في تنفيذ عمليات ذات فاعلية على الأرض وفي البحر والجو والفضاء من خلال نظم التحكم والسيطرة، فعلى العكس من التهديدات التقليدية الملموسة التي يمكن التنبؤ بها، يمكن أن تأخذ تهديدات الفضاء الإلكتروني شكلًا ومصدرًا افتراضيًا، وتفرض أخطارًا يصعب التنبؤ بها.

9. لقد لجأت الدول المتقدمة إلى حرب الفضاء الإلكتروني نتيجة مجموعة من الأسباب، أهمها تجنب العمل العسكري المباشر، ومحاولة تقليل الخسائر المادية والبشرية التي تترتب على العمل العسكري المباشر، وتجاوز الرأي العام الداخلي والخارجي الرافض للحروب التقليدية، وبالإضافة إلى ذلك فإنّ حرب الفضاء الإلكتروني ليست بحاجة إلى ساحات معارك كبيرة مثل المعارك التقليدية، فهجمات الفضاء الإلكتروني غير محددة المجال أو الأهداف، لأنها تتحرك عبر شبكات المعلومات والاتصال التي تتعدى الحدود الدولية، وتعتمد على أسلحة إلكترونية جديدة تلائم السياق التكنولوجي لعصر المعلومات، يتم توجيهها ضد المنشآت الحيوية.

10. تُعدّ حرب المعلومات والقرصنة الإلكترونية واستخبارات المصادر المفتوحة من أهم أدوات حرب الفضاء الإلكتروني. وقد أحدثت هذه الأدوات تحولًا بشأن إنتاج وتدفق وحرية تداول المعلومات دوليًا، وبرزت محاولات لاختراق أنشطة الدول السرية، فكان لا بدّ للدول من تعزيز دفاعاتها ضد خطر التعرض لهجمات الإلكترونية، والاتجاه إلى التحول من اتخاذ إجراءات وقائية ذات طابع دفاعي إلى تبني سياسات هجومية. ويحمل ذلك التوجه في طياته مخاطر عسكرة الفضاء الإلكتروني، وخصوصًا أنّ القدرة على السيطرة على هذا النوع من الأسلحة ضئيلة بالمقارنة مع الأسلحة التقليدية، وهناك مسألة صعوبة تحديد الأسلحة التي يمتلكها الآخرون، ومن ثم يصبح لدى المجتمع الدولي قدرة سريعة على التدخل لاحتواء التقدم في مجال هذه الأسلحة.
11. ساعدت الحرب النفسية الإلكترونية على ظهور النصوص الإلكترونية والوسائط الإعلامية المختلفة، التي باتت هي المجال الأوسع تطبيقًا في الصراعات الدولية المعاصرة، حيث أصبحت السيطرة على الساحات الافتراضية وخطوط الشبكة العنكبوتية والتحكم فيها الوسيلة الأكثر فاعلية لتحقيق الأهداف المرجوة، الأمر الذي أدى إلى تعدد أشكال حرب الفضاء الإلكتروني ووسائلها.
12. لقد تغير منظور الحرب جذريًا، حيث انتقلت من نسق «الحروب بين الدول إلى وسط الشعوب»، فقد كان الغرض من الحرب قديمًا هو تدمير الخصم، إمّا باحتلال أرضه أو الاستيلاء على موارده. أمّا الحروب الجديدة فتستهدف بالأساس التحكم في إرادة المجتمعات وخياراتها. ومن ثم، ظهرت للشعوب الأهمية المحورية لهذا النمط الجديد من الحروب،

سواء تعلق الأمر بالسكان المستهدَفين في أرضية المواجهة، أو بالرأي العام في الدولة التي تشنّ الحرب، أو بالرأي العام على الصعيدين الإقليمي والدولي.

13. لقد بات التعامل على المستوى النفسي يحتل الحيز الأكبر بين الأسلحة المستخدمة حاليًا في النظام الدولي الذي ظهر فيه فاعلون دون مستوى الدولة، وذلك للتأثير على وعي المستهدَفين، وأخذت فيه الحرب النفسية إطارًا أكثر شمولية، وأصبح الفضاء الإلكتروني من أبرز أدواتها المعروفة وأكثرها استخدامًا، وبات استخدام المعطيات الإلكترونية النفسية السرية والعلنية الوسيلة الأكثر فاعلية لإيجاد القناعات والآراء والاتجاهات التي تسهل تأمين المصالح، وتعين على إدارة الصراع وتحليله، حيث أُثبِتت فعالية الإنترنت كسلاح دعائي في الحرب النفسية، وأعطت الصراع بعدًا آخر من خلال التقنيات الدعائية الكثيفة التي استُخدِمت في العديد من الحروب، ولجأت إليها الأطراف المتصارعة.

14. أصبحت مواقع التواصل الاجتماعي تؤثر - بلا شك - في الأمن القومي للدول واستقرارها، وهو ما دعا العديد من المؤسسات القومية المهتمة بالأمن إلى دراستها ووضع الخطط الاستراتيجية للتعامل معها، وذلك لأنّ ما يتم نشره عبر تلك المواقع من أخبار ومعلومات غالبًا ما يفتقر إلى الصدق والدقة والمهنية، وتكون تلك الأخبار والمعلومات موجَّهة لتحقيق غايات خاصة، فعند التركيز في الخلفيات الأيديولوجية والفكرية والسياسية لمديري هذه المواقع نجد ذلك جليًا، بالإضافة إلى أنّ المحتوى المعلوماتي لهذه المواقع هو من أكثر المعلومات تداولًا بين الجمهور وخصوصًا الشباب، حيث تمكنت هذه المواقع من جذب أعداد هائلة من

المتصفحين في مدى زمني بسيط، متجاوزة بذلك قدرات أجهزة الإعلام التقليدية الأخرى بفارق كبير، وهو ما منحها قدرة كبيرة على التأثير في الساحة السياسية واتجاهات الرأي العام، وكذا في بث الأفكار والمعتقدات المتطرفة وخصوصًا لدى الشباب، وهو ما أدى إلى تغيير سياسي وأمني كبير، ومن ثم أصبحت هذه المواقع تُستخدَم لتهديد أمن الدول وزعزعة استقرارها.

التوصيات:

1. ضرورة تطوير استراتيجيات جديدة للوطن العربي، تتلاءم مع العصر السيبري الذي اختلفت فيه حسابات القوة والردع والحرب، هذا العصر الذي يُعتبَر فيه الإنترنت الإطار العام الحاكم لكافة تفاعلاته، سواء كانت شخصية أم عامة، عسكرية أم سياسية، اقتصادية أم اجتماعية.
2. التركيز على العلاقة بين الأمن الإلكتروني وقضايا التنمية الاقتصادية والاجتماعية والاستقرار السياسي، وصياغة استراتيجية عربية لمواجهة تصاعد الأخطار الإلكترونية، وأهمية تعاون كافة الفاعلين في مجتمع المعلومات العربي لترسيخ ثقافة عربية لأمن الفضاء الإلكتروني.
3. تعزيز أشكال التعاون في مجالات مكافحة المخاطر الإلكترونية من أجل تعزيز أمن الفضاء الإلكتروني، باعتباره مرفقًا دوليًا وتراثًا مشتركًا للإنسانية.
4. العمل على تطوير قدرة الدول العربية على إنتاج وتطوير أسلحة إلكترونية تُمكّنها من تحقيق أهدافها في الفضاء الإلكتروني، مع القدرة على تطوير تقنيات ذكية قادرة على تتبع مصادر الهجمات الإلكترونية ومعرفة الطرف المعتدي.

5. العمل على تطوير برامج حماية إلكترونية في مواجهة الهجمات الإلكترونية التي قد تتعرض لها البنى التحتية الاستراتيجية.
6. بناء شراكات بين الدولة والقطاع الخاص لتطوير البنية التحتية من ناحية، والتأكد من سلامة إجراءات التأمين المُتَّبَعة للحد من الهجمات الإلكترونية.
7. العمل على رفع جاهزية الدولة لإدارة عمليات إلكترونية تشمل مهاجمة شبكات الحاسب الآلي إذا دعت الحاجة إلى ذلك، والدفاع عن شبكاتها الخاصة واستطلاع الشبكات الأخرى.
8. ضرورة العمل على إعداد برامج توعوية حول أمن المعلومات الإلكترونية، نظرًا لأهميتها في مواجهة الحرب الإلكترونية.
9. ابتكار نظام تعليمي متقدم، يبدأ من مرحلة الطفولة، ويدعم الابتكار ويهتم بتدريس مجالات البرمجة والتصميم والذكاء الاصطناعي وغيرها من التكنولوجيات المتقدمة.
10. تشريع قوانين تحافظ على خصوصية الأفراد وتضمن حماية حياتهم الشخصية، وتمنع في الوقت نفسه ارتكاب الجرائم الإلكترونية وتحاسب عليها.

المراجع

أ. المراجع باللغة العربية:

الكتب:

- إبراهيم، خالد، (2008)، أمن المعلومات الإلكترونية، الإسكندرية، الدار الجامعية للنشر.
- أبـو زيـد، فـاروق، (1985)، فـن الخـبر الصـحفي، جـدة، دار الشـروق للنشـر والتوزيـع والطباعة.
- أحمـد، أبـو بكـر سـلطان، (2002)، التحـول إلـى مجتمـع معلومـاتي: نظـرة عامـة، أبـو ظبـي، مركز الإمارات للدراسات والبحوث الاستراتيجية.
- أحمـد، جمـال محمـد، (2015)، الإعـلام والتوجهـات الدوليـة الراهنـة، عمـان، دار غيـداء للنشر والتوزيع.
- الأشـرم، صـلاح الـدين، (1988)، الحـرب الإلكترونيـة مـن الحـرب العالميـة الأولـى إلـى حرب النجوم، دمشق، طلاس للدراسات والنشر.
- آل سـعود، نـايف ثنيـان، (2002)، تكنولوجيـا الاتصـال وأثرهـا في تطـور وسـائل الإعـلام وتداول المعلومات، الرياض، مطبعة سفير.
- ألبرت، ديفيد، (2006)، حـرب المعلومـات الدفاعيـة، الولايـات المتحـدة الأمريكيـة، مركـز القيادة المتقدمة والتكنولوجيا التابع لمعهد الدراسات الاستراتيجية.
- أولمـان، هـارلان، بـي ويـد، جيمس بـي، (2000)، دراسـات عالميـة: الهيمنـة السـريعة ثـورة حقيقيــة في الشــؤون العســكرية، أبــو ظبــي، مركــز الإمــارات للدراســات والبحــوث الاستراتيجية.

- إيفين، شموئيل، (2011)، مراجعة كتاب حرب الفضاء الإلكتروني: اتجاهات وتأثيرات على إسرائيل، ترجمة: محمود محارب، الدوحة، المعهد العربي للأبحاث ودراسة السياسات.
- بارون، وآخرون، (2017)، دراسة الشبكات الداعمة والمعارضة للدولة الإسلامية في العراق وسورية عبر تويتر، واشنطن، معهد أبحاث RAND للأمن القومي.
- باكير، علي حسين، (2012)، الحروب الإلكترونية في القرن الحادي والعشرين، قطر، مركز الجزيرة للدراسات.
- البداينة، ذياب، (2002)، الأمن وحرب المعلومات، عمان، دار الشروق، 2002.
- بدران، عباس، (2010)، الحرب الإلكترونية: الاشتباك في عالم المعلومات، بيروت، مركز دراسات الحكومة الإلكترونية.
- برعام، جيل، (2013)، تأثير تطور تكنولوجيا الحرب السبرانية على بناء القوة في إسرائيل، ترجمة: يولا البطل، فلسطين، مؤسسة الدراسات الفلسطينية.
- برم، عبد الكريم، (2010)، التقنية في الحرب: البعد الإلكتروني، أبو ظبي، مركز الإمارات للدراسات والبحوث الاستراتيجية.
- البريدي، عبد الله، (2011)، أسرار الهندسة الاجتماعية: نحو ابتكار أدوات جديدة لزيادة ذكائنا الجمعي، الرياض، وزارة الثقافة والإعلام السعودية.
- البصيلي، جاسم، (1989)، الحرب الإلكترونية: أسسها وأثرها في الحروب، بيروت، المؤسسة العربية للدراسات والنشر.
- بيلي، أولغا جوديس، وآخرون، (2009)، فهم الإعلام البديل، ترجمة علا أحمد صالح، القاهرة، مجموعة النيل العربية.
- جاسم، جعفر، (2010)، حرب المعلومات بين إرث الماضي وديناميكية المستقبل، عمان، دار البداية للنشر والتوزيع.
- الجهيني، منير، (2006)، أمن المعلومات الإلكترونية، الإسكندرية، دار الفكر الجامعي.

- حارص، صابر، (2008)، الإعلام العربي والعولمة الإعلامية والثقافية والسياسية، القاهرة، العربي للتوزيع والنشر.
- حسين، فاروق، (2002)، الإنترنت: شبكة المعلومات العالمية، مصر، هلا للنشر والتوزيع.
- خالد، محمد، (1990)، الحرب الإلكترونية، بغداد، موسوعة علوم سلسلة الكتاب العلمي العسكري.
- خليفة، إيهاب، (2016)، حروب مواقع التواصل الاجتماعي، القاهرة، دار العربي للنشر.
- خليفة، إيهاب، (2017)، القوة الإلكترونية: كيف يمكن أن تدير الدولة شؤونها في عصر الإنترنت، القاهرة، دار العربي للنشر.
- الخليفة، عمر، (2000)، علم النفس والمخابرات، بيروت، المؤسسة العربية للدراسات والنشر.
- خليل، عادل علي، (2002)، الحرب الإلكترونية من الحرب العالمية الأولى إلى حرب الخليج، القاهرة، دار الهلال.
- رحومة، علي محمد، (2007)، الإنترنت والمنظومة التكنو -اجتماعية، بيروت، مركز دراسات الوحدة العربية.
- رسلان، أحمد فؤاد، (1968)، نظرية الصراع الدولي، القاهرة، الهيئة المصرية العامة للكتاب.
- الرزو، حسن مصطفى، (2012)، الجاهزية الإلكترونية للبلدان العربية وانعكاساتها المحتملة على فرص تفعيل بيئة اقتصاد المعرفة، بيروت، مركز دراسات الوحدة العربية.
- الرزو، حسن مظفر، (2008)، حرب المعلومات الإعلامية: عن كتاب ثورة الصورة والمشهد الإعلامي وفضاء الواقع، بيروت، مركز دراسات الوحدة العربية.
- الرزو، حسن مظفر، (2007)، الفضاء المعلوماتي، بيروت، مركز دراسات الوحدة العربية.

- السعدون، حميد حمد، (2011)، التنمية السياسية والتحديث في العالم الثالث، عمان، الذاكرة للنشر والتوزيع.
- السعدي، كمال، (1997)، الحرب الإلكترونية، بيروت، المؤسسة العربية للدراسات والنشر.
- سلامة، صفات، (2011)، أسلحة حروب المستقبل بين الخيال والواقع، أبو ظبي، مركز الإمارات للدراسات والبحوث الاستراتيجية.
- سليمان، هاني، (2014)، نوايا خفية: الحرب الأمريكية على داعش، الدوحة، المركز العربي للبحوث والدراسات.
- سنو، مي العبد الله، (2006)، التلفزيون وقضايا الاتصال في عالم متغير، بيروت، دار النهضة العربية.
- السويدي، جمال سند، (2013)، وسائل التواصل الاجتماعي ودورها في التحولات المستقبلية: من القبيلة إلى الفيسبوك، أبو ظبي، مركز الإمارات للبحوث والدراسات الاستراتيجية.
- سينجر، بيتر، (2010)، الحرب عن بعد: دور التكنولوجيا في الحرب، أبو ظبي، مركز الإمارات للدراسات والبحوث الاستراتيجية.
- الشمسي، إبراهيم أحمد، (1999)، صناعة الخبر الصحفي، الشارقة، مطبعة المعارف.
- شوقي، حسام، (2003)، حماية وأمن المعلومات على الإنترنت، بيروت، دار الكتب العلمية.
- الصادق، رابح، (2004)، الإعلام والتكنولوجيا الحديثة، الإمارات، دار الكتاب الجامعي.
- صالح، سليمان، (2003)، ثورة الاتصال وحرية الإعلام، الكويت، دار الفلاح.
- العالم، صفوت، (2005)، دور وسائل الإعلام في الإصلاح السياسي، القاهرة، مركز الأهرام للدراسات السياسية والاستراتيجية.

- عبد الحميد، صلاح، (2015)، الإعلام والفضاء الإلكتروني، الجيزة، أطلس للنشر والإنتاج الإعلامي.
- عبد الصادق، عادل، (2009)، الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، القاهرة، مركز الدراسات السياسية والاستراتيجية.
- عبد الصادق، عادل، (2013)، الحملات الإلكترونية: محاولة الانتقال من الفعل الفردي إلى الجماعي، مصر، المركز العربي لأبحاث الفضاء الإلكتروني.
- عبد الصادق، عادل، (2011)، الدبلوماسية ومعركة القوة الناعمة بين الولايات المتحدة وإيران، القاهرة، مركز الأهرام للدراسات السياسية والاستراتيجية.
- العبد، نهى عاطف، (2009)، الإعلام الدولي، القاهرة، الدار العربية للنشر.
- عجوة، علي، (1999)، مقدمة في وسائل الاتصال، جدة، مكتبة مصباح.
- عليان، ربحي، (2006)، مجتمع المعلومات والواقع العربي، عمان، دار جرير للنشر والتوزيع.
- عليوة، السيد، (1988)، إدارة الصراعات الدولية: دراسة في سياسات التعاون الدولي، القاهرة، الهيئة المصرية العامة للكتاب.
- غيطاس، جمال، (2007)، الحرب وتكنولوجيا المعلومات، القاهرة، دار نهضة مصر.
- فريدمان، لورنس، (2000)، دراسات عالمية: الثورة في الشؤون الاستراتيجية، أبو ظبي، مركز الإمارات للدراسات والبحوث الاستراتيجية.
- قنديلجي، عامر إبراهيم، وآخرون، (2000)، مصادر المعلومات من عصر المخطوطات إلى عصر الإنترنت، عمّان، دار الفكر للطباعة والنشر والتوزيع.
- كامل، محمود عبد الرؤوف، (1995)، مقدمة في علم الإعلام والاتصال بين الناس، القاهرة، جامعة القاهرة، مكتبة نهضة الشرق.
- كلارك، ريتشارد، (2012)، حرب الفضاء الإلكتروني: التهديد التالي للأمن القومي وكيفية التعامل معه، أبو ظبي، مركز الإمارات للبحوث والدراسات الاستراتيجية.

- كوبلاند، توماس، (2003)، ثورة المعلومات والأمن القومي، سلسة دراسات عالمية، أبو ظبي، مركز الإمارات للدراسات والبحوث الاستراتيجية.
- متولي، مصطفى، (2001)، أمن إسرائيل: الجوهر والأبعاد، أبو ظبي، مركز الإمارات للدراسات والبحوث الاستراتيجية.
- مساعد، كمال، (2005)، منظومة الدفاع الإسرائيلية: المتغيرات والمواجهة المستقبلية، بيروت، مؤسسة ماجيك لاين.
- المشاط، عبد المنعم، (1995)، تحليل وحل الصراعات: الإطار النظري، القاهرة، المركز القومي لدراسات الشرق الأوسط.
- مكاوي، حسن، (1993)، تكنولوجيا الاتصال الحديثة في عصر المعلومات، القاهرة، الدار المصرية اللبنانية.
- مكاوي، حسن، (2009)، نظريات الإعلام، الدار العربية، القاهرة.
- ناي، جوزيف إس، (2015)، مستقبل القوة، ترجمة: أحمد عبد الحميد نافع، القاهرة، المركز القومي للترجمة.
- النجيفي، سالم توفيق، (2010)، اقتصاد العولمة: مقاربات اقتصادية للرأسمالية وما بعدها، بيروت، دار النفائس للطباعة والنشر.
- هارتلي، جون، وآخرون، (2007)، الصناعات الإبداعية، ترجمة بدر السيد سليمان الرفاعي، الكويت، عالم المعرفة.
- هيرش، سيمور، (2016)، قتل أسامة بن لادن والتدخل في سورية، ترجمة محمد جياد الأزرقي، بيروت، الدار العربية للعلوم.
- الوردي، زكي حسن، المالكي، مجبل لازم، (2002)، مصادر المعلومات وخدمات المستفيدين في المؤسسات المعلوماتية، عمان، مؤسسة الوراق للنشر والتوزيع.
- اليحياوي، يحيى، (2004)، أوراق في التكنولوجيا والإعلام والديمقراطية، بيروت، دار الطليعة للنشر.

الدوريات:

- إبراهيم، سعد الدين، (2012)، عوامل قيام الثورات العربية، بيروت، مجلة المستقبل العربي، العدد 399، مايو.
- إبراهيم، يسري خالد، (2011)، الحرب النفسية الإلكترونية، بغداد، مجلة الباحث الإعلامي، العدد 13، تموز.
- أبو طالب، أحمد، (2012)، القرصنة السياسية عبر الفضاء، القاهرة، مجلة السياسية الدولية، العدد 187 يناير.
- أبو ليلة، سعاد محمود، (2012)، دورة القوة: ديناميكيات الانتقال من الصلبة إلى الناعمة إلى الافتراضية، القاهرة، مجلة السياسة الدولية، العدد 188 أبريل.
- أحمد، عبد الخالق محمد، (2014)، الهندسة الاجتماعية، الخرطوم، مجلة المال والاقتصاد، العدد 75، سبتمبر.
- بابكر مصطفى، معتصم، (2014)، أيديولوجيا شبكات التواصل الاجتماعي وتشكيل الرأي العام، مركز التنوير، الخرطوم.
- بدوي، منير، (1997)، مفهوم الصراع: دراسة في الأصول النظرية للأسباب والأنواع، القاهرة، مجلة دراسات مستقبلية، العدد 3، يوليو.
- بنور، بيار، (2015)، البنى التحتية الاستراتيجية والحرب الإلكترونية، تونس، مجلة مستقبليات، العدد 3 يوليو.
- بهاز، حسين، (2010)، مقاربة نظرية لظاهرة الصراع الدولي، الجزائر، مجلة دفاتر السياسة والقانون، العدد 3، جوان.
- بورجيلي، ريمون، (2005)، التكنولوجيا الحديثة في المجالات العسكرية، مجلة الجيش اللبناني، بيروت، العدد 236، شباط.
- جواد، أنمار موسى، (2016)، حرب الفضاء الإلكتروني المفهوم والأدوات والتطبيق، الخرطوم، مجلة العلوم القانونية والسياسية، العدد 2 فبراير.

- الخوري، تانيا، (2011)، كلنا شهود عيان: ربيع العرب بالصور والحروب الإلكترونية، فلسطين، مجلة الدراسات الفلسطينية، العدد 88، أكتوبر.
- راضي، زاهر، (2003)، استخدام مواقع التواصل الاجتماعي في العالم العربي، عمان، مجلة التربية، جامعة عمان الأهلية، العدد 15.
- الراوي، بشرى جميل، (2012)، دور مواقع التواصل الاجتماعي في التغيير: مدخل نظري، بغداد، مجلة الباحث، العدد 18 آب.
- السعدون، حميد حمد، (2012)، الحرب الإلكترونية جبهة قتال جديدة بين إيران وخصومها، بغداد، مجلة أوراق دولية، العدد 218، تشرين الأول.
- السبيعي، ناصر عبد الله، (2013)، المصادر المفتوحة وأهميتها كوسيلة استخبارية، الرياض، مجلة الدفاع العسكرية، العدد 110 كانون الأول.
- السامرائي، إيمان فاضل، (2003)، مصادر المعلومات الإلكترونية وتأثيرها على المكتبات، تونس، المجلة العربية للمعلومات، مجلد 14، العدد 1، يناير.
- السيد، دلال محمود، (2016)، حرب المعلومات، القاهرة، مجلة لغة العصر، العدد 16 يناير.
- شلبي، مجدي، (2002)، أمن المعلومات، الإمارات، مجلة درع الوطن، العدد 378 تشرين الثاني.
- شميسي، وداد، (2014)، الحوار الإلكتروني والفضاء العام الافتراضي، الجزائر، مجلة العلوم الإنسانية، العدد 41، حزيران.
- شواريتو، وينن، (2008)، حرب المعلومات، مجلة الدفاع الوطني، الولايات المتحدة الأمريكية، مركز القيادة المتقدمة والتكنولوجيا التابع لمعهد الدراسات الاستراتيجية.
- الشوري، أحمد، (2015)، هل تشكل مواقع التواصل الاجتماعي تهديدًا للأمن القومي؟، القاهرة، مجلة السياسة الدولية، العدد 210، سبتمبر.

- شيخاني، سميرة، (2010)، الإعلام الجديد في عصر المعلومات، دمشق، مجلة جامعة دمشق، العدد 26، تشرين الثاني.
- صقر، أمل، (2014)، مخاطر واقعية: كيف يهدد التواصل الاجتماعي الأمن الوطني؟، القاهرة، مجلة السياسة الدولية، العدد 208، أغسطس.
- عبد الصادق، عادل (2012)، القوة الإلكترونية: أسلحة الدمار الشامل في عصر الفضاء الإلكتروني، القاهرة، مجلة السياسة الدولية، العدد 188 أبريل.
- عبد الصادق، عادل، (2015)، الفضاء الإلكتروني وإشكالية نظرية العلاقات الدولية، القاهرة، مجلة السياسة الدولية، العدد 200، أبريل.
- عبد الصادق، عادل، (2014)، الاستخبارات الجديدة: إشكالية التجسس الإلكتروني في العلاقات الدولية، القاهرة، مجلة السياسة الدولية، العدد 195، يناير.
- عثمان، أحمد زكي، (2017)، تأثيرات القدرات السيبرانية في الصراعات الإقليمية، القاهرة، مجلة السياسة الدولية، العدد 209، أبريل.
- علو، أحمد، (2011)، الروبوت جندي حروب المستقبل، مجلة الجيش اللبناني، بيروت، العدد 317 تشرين الثاني.
- علي، نبيل، (2001)، الثقافة العربية وعصر المعلومات، الكويت، مجلة عالم المعرفة، العدد 265 كانون الثاني.
- العليان، محمد، (2011)، في ذكرى حرب لبنان تموز 2006: كتب أمريكية تؤكد نجاح حزب الله في الحرب غير المتماثلة، بيروت، مجلة الفلق، العدد 13 أغسطس.
- ليبيك، مارتن، (2007)، ما هي حرب المعلومات، مجلة الدفاع الوطني، الولايات المتحدة الأمريكية، مركز القيادة المتقدمة والتكنولوجيا التابع لمعهد الدراسات الاستراتيجية.
- محمود، خالد وليد، (2013)، الهجمات عبر الإنترنت ساحة الصراع الإلكتروني الجديدة، قطر، مجلة سياسات عربية، العدد 5، تشرين الثاني.

- نصر، نجيب، (2001)، المحاربون الروبوت في معارك المستقبل، مجلة الدفاع، القاهرة، العدد 180 يوليو.

ب. المراجع باللغة الإنجليزية:

- Arsenio T. Gumahad, Cyber Troops and Net Wars: The Profession of Arms in The Tnformation Age, Air War College, April 1996.
- David E. Sanger, Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power (New York: Crown, 2012).
- Danial t. Kuehl, the radar blinded: the USAF and Electronic warfare, 1945-1955. Dissertation (Durham, NC: Duke University) 1992.
- Diego Rafael Canabarro,« Reflection on the fog of Cyber War», National Center for Digital Government, Policy working Paper No.13:001, March 1, 2013.
- Eric Schmitt, «why Iraqi Battle Threat Fizzled: Allied Strengths and Enemy Weaknesses», the New York time, March 4, 1991.
- Gabriel Weismann, Terror on The Internet: The News Arena, The New Challenges, United States institute of peace press, 2006.
- Jenn M. Williamson, Information Operation: Computer network attack in the 21st century, US Army War College, 2002.
- Joshuo, Kuccra «US Army speeds fielding of armed robots to iraq» jane's defense weakly, vol.42. no 5: February 2, 2005.
- Justin Pope, «looking to Iraq, military robots focus on lessons of Afghanistan» Detroit news, January 12, 2003.
- K. Saalbach,« Cyber War, Methods and Practice», Version 9.0, University of Osnabruck-17 Jun 2014
- Martin C. Libicki, Conquest in Cyber Space: National Security and Warfare, New York, Cambridge University press, 2007.

- Mario De Archangelis, Electronic Warfare (pool, UK Blandford Press, 1985).
- Mazarr, M, s., D. and Blackwell, jr. 1993, Desert storm: The Gulf war and what we Learned, Westview Press, Boulder, Co.
- Michael Chertoff, The Cyber Domain and The Evolution of Smart Power, in: Dealing with Today`s Asymmetric Threat to U.S and Global Security, Symposium Three, March 24, 2009.
- NATO, open source- intelligence- hand book, 2001.
- Nazli, Choucri, Cyber Politics in International Relation, Cambridge MIT Press, 2012.
- Peter Margulies,» Sovereigntyand Cyber Attacks: Technology's Challenge to the Law of State Responsibility», Melbourne Journal of International Law, Vol.14.2013.
- Richard o. hundley, past revolutions future transformations,2010.
- Robert finkelstein, «military robotics: malignant machines or the path to peace», paper presented at the military robotics conference, institute for defense and government advancement, Washington, DC, April 10_12, 2016.
- Richard K. Betts. Conflict after the Cold War: Arguments on Causes of War and Peace, 2nd ed. (New York: Longman, 2002) university press 2013.
- Staff Barbara, «satellites paved way to victory», janes defense weekly, March 9, 1991.
- Time Jordan, Cyber Power: The Culture and Politics of Cyberspace and the internet, Rutledge, 2000.
- Tom Quinn and John Porter, «EV and C3 countermeasures- the official view» journal of electronic defense (November-December). 2001

- Zimet E.and C. L. Barry,« Military services Overview, Cyber power and National Security», National Defense University Press, Washington, DC, USA,2009.

ت. المواقع الإلكترونية:

- الرميح، يوسف، (2015)، الإرهاب في شبكات التواصل الاجتماعي، مجلة الجزيرة الإلكترونية، عبر الرابط الإلكتروني:

http://www.al-jazirah.com/2015/20150323/ar2.htm

- ناي، جوزيف، (2005)، الحرب والسلام في الفضاء الإلكتروني، بحث منشور على شبكة الإنترنت، عبر الرابط الإلكتروني:

http//: www.project-syndicate.org/commentary/presedant-push-gose-soft/Arabic.

- برادلي، سايمون، نحو استبدال البشر في ساحات المعارك بالأسلحة المُستقلة، مدونة مستجدات سويسرية عبر الرابط الإلكتروني: https://www.swissinfo.ch/ara

- حسان، أيمن، (2017)، دور مواقع التواصل الاجتماعي في نشر الفكر المتطرف، ورقة بحثية مقدمة للمركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات عبر الموقع الإلكتروني: http://www.europarabct.com

- اليحياوي، يحيى، 2010، حرب المعلومات، على الموقع الإلكتروني للكاتب يحيى اليحياوي: www.elyahaoui.org/medias_war.htm

- William. J. Broad, John Markoff and David E. Sanger, «Israeli Test on Worm Called Crucial in Iran Nuclear Delay», The New York Times (15 Jan 2011), online e-article, http://www.nytimes.com/16/01/2011/world/middleeast/16stuxnet.html_r=1&pagewanted=all
- Tims, R. (2001), Social Engineering: Policies and Education a Musthttp://www.sons.org/infosecFAO/social/policies.html

- Joseph S. Nye, Cyber War and Peace, project syndicate, 10 April 2012, http//: www.project-syndicate.org/commentary/cyber-war-and-peace.
- Joseph S. Nye, Cyber Insecurity, project syndicate, Dec10, 2008, http//: www.project-syndicate.org/commentary/cyber-insecurity.
- Misha Glenny, The Cyber Arms Race Is On, October 23, 2011, www.post-gexzettle.com/p8/113849/-mty .
- Joseph S. Nye, Jr, «The Changing Nature of World Power», Political Science Quarterly, Vol. 105, No. 2 (Summer, 1990), Published by: The http://www.jstor.org/stable/2151022.
- Ernest J. Wilson, III, «Hard Power, Soft Power, Smart Power», Annals of the American Academy of Political and Social Science, Vol. 616, Public Diplomacy in a Changing World (Mar. 2008), pp. 110-124, Published by:
- URL: http://www.jstor.org/stable/25097997

ث. الرسائل الجامعية والندوات:

- الدعجة، هايل ودعان، (2008)، الإعلام والإرهاب، الأردن، ورقة مقدمة إلى مؤتمر جامعة الحسين بن طلال الدولي حول الإرهاب في العصر الرقمي بتاريخ 10_12 / 7 / 2008.
- زريقات، مراد بن علي، (2008)، الرأي العام الإلكتروني: تأثير وسائل الاتصال الإلكترونية في الرأي العام، ورقة عمل مقدمة ضمن ندوة الجرائم الإلكترونية، جامعة نايف العربية للعلوم الأمنية 2_4/ 6/ 2008.
- طه، وليد رشاد، (2007)، الجماعات المتشكلة في الفضاء العالمي: بناؤها ومضامين تفاعلاتها الاجتماعية، رسالة ماجستير غير منشورة، كلية الآداب، جامعة عين شمس.

- عبد الصبور، سماح، (2013)، القوة الذكية في السياسة الخارجية: دراسة في أدوات السياسة الخارجية الإيرانية تجاه لبنان منذ 2005، رسالة مقدمة لنيل درجة الماجستير، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة.
- علي، نوران شفيق، (2014)، الفضاء الإلكتروني وأنماط التفاعلات الدولية: دراسة في أبعاد الأمن الإلكتروني، رسالة ماجستير غير منشورة، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية.
- محمود، زكريا، (2005)، ورقة في الجريمة المعلوماتية وأساليب التأمين، سلطنة عمان، المؤتمر الدولي لأمن المعلومات الإلكترونية.



د. ماجد محمد الحنيطي

تكنولوجيا الصراعات الدولية المعاصرة

يحاول هذا الكتاب تسليط الضوء على الثورة المعلوماتية الضخمة التي شهدتها القطاعات الأمنية والعسكرية والسياسية حول العالم، وبيان أثر الفضاء الإلكتروني بجميع مكوناته في الصراعات الدولية المعاصرة.

فقد أحدثت التطورات الفكرية والصناعية التي وصل إليها الإنسان ثورة كبيرة في وسائل القتال والصراعات بين البشر، وهو ما أدى إلى تغيرات جذريّة في المفاهيم؛ فبعد أن كانت الجيوش الجرّارة والحشود والقذائف تمثّل لغة الصراع والقوة، دخلت وسائل الاتصال الإلكتروني ساحة الصراع لتضيف بعداً جديداً من أبعادها؛ يتمثل بحرب الفضاء الإلكتروني (Electronic Warfare).



